XenApp and XenDesktop 7.6

Oct 17, 2016

What's new

Long Term Service Release (LTSR)

Feature Pack 3: Install and upgrade

Feature Pack 3: Fixed issues

Known issues

Features not in this release

System requirements

Technical overview

Concepts and components

Active Directory

Fault tolerance

Delivery methods

Reference Architectures

Design Guides

Implementation Guides

New deployments

Prepare to install

Prepare the virtualization environment: VMware

Prepare the virtualization environment: Microsoft System Center Virtual Machine Manager

Prepare for using Microsoft System Center Configuration Manager

Install using the graphical interface

Install using the command line

Create a Site

Install or remove Virtual Delivery Agents using scripts

Machine catalogs

Delivery groups

XenApp published apps and desktops

VM hosted apps

VDI desktops

Remote PC Access

App-V

Local App Access and URL redirection

Server VDI

Remove components

Upgrades and migration

Upgrade a deployment

Migrate XenApp 6.x

Migrate XenDesktop 4

Security

Getting Started with Citrix XenApp and XenDesktop Security

Security best practices and considerations

Delegated Administration

Smart cards

SSL

Policies

Work with policies

Policy templates

Create policies

Compare, prioritize, model, and troubleshoot policies

Default policy settings

Policy settings reference

Printing

Printing configuration example

Best practices, security considerations, and default operations

Print policies and preferences

Provision printers

Maintain the printing environment

Licensing

What's new

Mar 03, 2016

In this article:

Feature Pack 3

The Feature Pack 3 release includes the following new enhanced features.

For install and upgrade instructions, see Install and upgrade Feature Pack 3 components.

Fixed Issues

Virtual Delivery Agent (VDA)

The updated VDA standalone package adds:

- **Support for Windows 10** Enterprise Edition, in the Standard VDA for Windows Desktop OS.

Universal Print Server

The updated Universal Print Server package adds:

- **Support for Windows Server 2012 R2**.

HDX technologies

The following new and enhanced HDX technologies features are included in the Feature Pack 3 VDA and managed using the updated Group Policy Management package:

- **Enhancements to Thinwire Compatibility Mode.** This mode uses an updated encoder that improves the display performance of simple graphical interfaces, for example in MS Excel and MS Word, without requiring the use of a resource-intensive video codec. For more information, see Thinwire Compatibility Mode.
- **Support for signature devices and drawing tablets.** Administrators can set a policy to enable devices for client-side polling and set optimization modes as part of that policy. This means that users can work effectively in wide area networks with devices such as Wacom signature pads and tablets within XenApp and XenDesktop sessions. For more information, see USB devices policy settings.
- **Video fallback prevention policy.** Enables administrators to have more control over server-side and client-side fetching and rendering of multimedia content. For example, if a user's device cannot play a video locally, a new setting allows the

administrator to control whether the video is automatically rendered on the server, or prevented and a message displayed to the user. For more information, see Multimedia policy settings and Flash Redirection policy settings.

- **Minimum version checking for Flash redirection.** For client devices accessing VDAs using Receiver for Windows and Receiver for Linux. This gives administrators greater control over specifying minimum versions required for Flash redirection. For more information on how to specify minimum versions, see Flash Redirection.
- **Smart card virtual channel improvements.** Includes support for smart card reader plug-and-play with Receiver for Windows 4.3, virtual smart cards (Microsoft Windows Trusted Platform Module-based virtual smart cards), and performance improvements. For more information on deploying smart cards, see Smart cards, and Virtual Smart Card Overview in the Microsoft Windows TechCenter.
- **Framehawk virtual display channel integration with the VDA.** The Framehawk virtual display channel is integrated into the standalone VDA package. With Framehawk integrated into HDX technology, Citrix provides a smooth and intuitive user experience in conditions where remote workspace users previously experienced poor interactivity, such as on wireless connections with high packet loss or congestion. For more information, see the HDX Framehawk virtual channel administrator guide.
- **Full-screen app support for HDX 3D Pro VDI.** The Virtual Delivery Agent (VDA) for HDX 3D Pro supports full-screen apps including 3D and gaming apps within single monitor ICA sessions.
- **Custom hotkey configuration for lossless compression.** With HDX 3D Pro, the administrator can configure a registry setting to set a custom keyboard shortcut to override the default (ALT+SHIFT+1). Users can instantly switch between lossy and visually lossless compression, or between lossy and lossless compression using a custom hotkey. For more information, see GPU acceleration for Windows Desktop OS.
- **Call Home.** In this version of Call Home, administrators can run a PowerShell cmdlet (**Start-TelemetryUpload**) to extract VDA diagnostic information. You can use the cmdlet to either create a local ZIP file, which you can email to your support representative, or you can use credential information combined with a Support Service Request (SR) number to automatically upload the information to Citrix Insights Services. This enables administrators and support representatives to identify and troubleshoot VDA-related issues. The PowerShell cmdlet is supplied with the VDA installer in FP3.
- **Enhanced HDX printer support and configuration.** Includes always-on logging for the print server and printing sub-system on the VDA, and the option to join the Citrix Customer Experience Improvement Program (CEIP). For more information, see Install using the command line and Best practices, security considerations, and default operations.
- **Updated Policy templates.** This feature pack delivers new policy templates for High Server Scalability and Optimized for WAN, and replaces the High Definition User Experience template with the Very High Definition template. For more information, see Policy templates.
- **32-bit cursor support.** Delivers an improved user experience in 3D applications which rely on custom cursors.
- **Desktop Composition Redirection (DCR).** DCR is disabled by default.

StoreFront 3.0.1

The updated StoreFront package adds:

- **Support for Transport Layer Security (TLS) 1.0 and 1.1.** Secure Sockets Layer (SSL) 3.0 is **not** supported and Citrix strongly recommends that you do not use it.

See StoreFront documentation for more information.

Linux Virtual Desktop 1.1

You can create Linux virtual desktops based on SUSE and Red Hat distributions. Prepare your Linux virtual machines, install the new Linux VDA software on them, configure your Delivery Controller, and then use Studio to make the desktops available to users. For more information, see the following documents:

PDF Installation guide for SUSE

PDF Installation guide for Red Hat

Feature Pack 2

The Feature Pack 2 release includes the following new and enhanced features.

StoreFront 3.0

StoreFront includes the following new features and enhancements.

Updated StoreFront management console

Support for the unified Receiver experience. StoreFront 3.0 delivers centralized customization and branding of your end users' applications and desktop selection experience to Receiver users. Your company can customize the interface to reflect your logo, colors, and so forth. Some of the new Receiver and StoreFront features:

- **Simplified application organization**. Familiar and consistent application selection experience for use.
  - Featured app groups. Administrator configured applications that are logically grouped and advertised to users in the applications selection experience.
  - Folder view of applications. Return of Web Interface functionality in StoreFront.
  - Favorites. Easily add or remove applications to Favorites for quick access.
- **Server-managed user experience**. Application selection experience is server configured.
  - Change once, deploy everywhere. User application selection experience changes are made by the administrator on StoreFront server.
  - Consistent application selection experience for users. Any device running Receiver receives its application selection experience from the server as HTML5, providing for consistency as users move across smartphones, tablets, and desktop form factors.
  - Decouple the application selection experience from Receiver capabilities. Client upgrade without end user training or user experience impact; Support legacy user experience without legacy client cost.
- **Fit for purpose user experience customization options**. You select the appropriate level of customization.
  - Updated out-of-the-box user experience. Modernized end user application selection look-and-feel.
  - Server-configured branding customizations. You brand with corporate logos, color, and featured application groups.
  - Deeper customization and branding options. CSS and script APIs available to enable deeper levels of customization.
- **Use the StoreFront management console to do the following Receiver related tasks**:
  - Set Receiver for Web as the default for the store.
  - Create a Receiver for Web website.
  - Change website type.
  - Customize the website appearance.

See the Manage a Citrix Receiver for Web site articles.

- **Featured app groups management**. App groups are groups of applications that are related or fit in a specific category making them more easily discoverable. With Studio and the StoreFront management console you can define app groups using keywords, application names, or categories.

  See the Create and manage featured apps article.

XML service-based authentication

If you configure all of them; the event that occurs first will cause the unused session to end. Use PowerShell cmdlets to enable and disable this feature. For more information, see XML service-based authentication.

Support for HDX Real-Time Optimization Pack 1.8 for Microsoft Lync

HDX RealTime Optimization Pack includes the following new features and enhancements.

- Support for the Microsoft Skype for Business client in Lync UI mode, the Microsoft Lync 2013 client, and the Microsoft Lync 2010 client.
- Support for the Lync Server 2013 Autodiscover Service.
- Call Park and Call Pick Up in Lync 2010 client.
- Call forwarding and simultaneous ringing controls for Lync 2010 client
- Support for Mac.
- Kerberos authentication.
- Plus (+) symbol in the dial pad.
- Support for the Microsoft Windows 10 technical preview.

For information, see HDX RealTime Optimization Pack 1.8 for Microsoft Lync.

Session Recording

Session Recording includes the following new features and enhancements.

- You can specify the connection credentials to the database when installing the Session Recording Database component.
- You can test the connectivity of database during the installation of the Session Recording Database and Session Recording Server components and test the connectivity of the Session Recording Server during the installation of Session Recording Agent component.
- Microsoft Shared Management Objects is no longer requirement for Session Recording Database installation.
- Citrix Experience Improvement Program (CEIP) is integrated in Session Recording. For more information, see About the Citrix Customer Experience Improvement Program.

For more information, see Session Recording - for XenApp 7.6 FP1, FP2, and LTSR.

Linux Virtual Desktop

You can now create Linux virtual desktops based on SUSE and Red Hat distributions. Prepare your Linux virtual machines, install the new Linux VDA software on them, configure your Delivery Controller, and then use Studio to make the desktops available to users. For more information, see the latest documents in the Feature Pack 3 section above.

Framehawk Virtual Channel

Framehawk is a new ICA virtual channel that extends Citrix HDX technologies, a set of capabilities that work together to deliver a high-definition user experience of virtual desktops and applications.

The Framehawk virtual channel optimizes the delivery of virtual desktops and applications to users on broadband wireless connections. It is ideal for mobile devices under lossy network connections. With Framehawk integrated into the industry-leading HDX technology, Citrix provides a smooth and intuitive user experience in conditions where remote workspace users previously experienced poor interactivity, such as on wireless connections with high packet loss or congestion.

For more information, see the following document which contains information for both XenApp and XenDesktop 7.6 Feature Pack 3 and Feature Pack 2.

PDF Framehawk administrator guide

Director 7.6.300

This version of Director supports the Framehawk virtual channel and contains fixes for the following issues in that were present in Version 7.6.200. For more information on installing this component, see the Director documentation.

Fixed issues

Feature Pack 1

The Feature Pack 1 release includes the following new and enhanced features.

Session Recording

Session Recording allows you to record the on-screen activity, over any type of connection, from any server running XenApp subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback. For more information, see Session Recording - for XenApp 7.6 FP1, FP2, and LTSR.

Citrix Director 7.6.200

With Director 7.6.200, you can enable and disable the Session Recording policy from the User Details and Machine Details views. Use the Director console to create and activate Session Recording policies.

For more details about the integration of Session Recording and Director, see http://support.citrix.com/article/CTX142260. For more information about Session Recording, see Session Recording - for XenApp 7.6 FP1, FP2, and LTSR.

Citrix Licensing 11.12.1

Citrix Licensing Customer Experience Improvement Program (CEIP) and Call Home — Voluntary data collection programs in which Citrix products gather anonymous or identified configuration, performance, error, and usage data from your deployment and automatically send the data to Citrix. For more information, see Citrix Licensing Customer Experience Improvement Program (CEIP) and Call Home. Not supported with License Server VPX.

The Citrix Customer Experience Improvement Program (CEIP) gives you the opportunity to contribute to the design and development of Citrix products. When you enroll in the program, Citrix collects anonymous information about your deployment, which is used to improve product quality, reliability, and performance.

For more information, see About the Citrix Customer Experience Improvement Program.

Support for HDX Real-Time Optimization Pack 1.7 for Microsoft Lync

Citrix HDX RealTime Optimization Pack 1.7 for Microsoft Lync provides a highly scalable solution for delivering real-time audio-video conferencing and VoIP enterprise telephony through Microsoft Lync in XenDesktop and XenApp environments to users on Linux and Windows devices. The Optimization Pack leverages your existing Microsoft Lync infrastructure and interoperates with other Microsoft Lync endpoints running natively on devices.

For information, see HDX RealTime Optimization Pack 1.7 for Microsoft Lync.

XenApp 7.6 and XenDesktop 7.6

This product release includes the following new and enhanced features.

Session prelaunch and session linger

The session prelaunch and session linger features help users quickly access applications by starting sessions before they are requested (session prelaunch) and keeping application sessions active after a user closes all applications (session linger). These features are supported for Server OS machines only.

By default, session prelaunch and session linger are not used. A session starts (launches) when a user starts an application and remains active until the last open application in the session closes. You can enable the features for all users in a Delivery Group or only for specified users.

There are several ways to specify how long an unused session remains active if the user does not start an application: a configured timeout and two server load thresholds. You can configure all of them; the event that occurs first will cause the unused session to end.

For more information, see Configure session prelaunch and session linger.

Support for unauthenticated (anonymous) users

When creating or editing Delivery Groups containing Server OS machines, you can now allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. For example, when users access applications through kiosks, the application may require credentials, but the Citrix access portal and tools do not.

When you configure the Delivery Group, you can grant access to authenticated users, unauthenticated users, or both. When you grant access to unauthenticated (anonymous) users, you must provide an unauthenticated StoreFront store.

For more information, see Users.

Connection leasing

To ensure that the Site database is always available, Citrix recommends starting with a fault-tolerant SQL Server deployment by following high availability best practices from Microsoft. However, network issues and interruptions may prevent Delivery Controllers from accessing the database, resulting in users not being able to connect to their applications or desktop.

The connection leasing feature supplements the SQL Server high availability best practices by enabling users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available.

Although users may have a large number of published resources available, they often use only a few of them regularly.

When you enable connection leasing, each Controller caches user connections to those recently used applications and desktops during normal operations (when the database is available). If the database becomes unavailable, the Controller enters leased connection mode and "replays" the cached operations when a user attempts to connect or reconnect to a recently used application or desktop from StoreFront.

For more information, see Connection leasing.

Application folders

You can organize applications in folders, which makes it easier to administer large numbers of applications in Studio.

By default, applications in a Delivery Group appear in a single folder. From the Delivery Group display in Studio, you can create additional folders and move applications into them. Moving, nesting, and renaming folders are easy drag-and-drop operations; you can also use Actions menu items. Additionally, you can specify folder destinations and create new folders when you add applications to a Delivery Group.

For more information, see Manage application folders.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a Site running XenApp 7.6 (or a later supported release). This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp Site.

After you install the XenApp 7.6 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.6 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Windows Server OS for use in the new Site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new Site. By tailoring the files, you can import policy and application settings into your XenApp 7.6 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.6 Controller, which import settings from the XML files to the new XenApp Site.
- Reconfigure the new Site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Citrix Customer Experience Improvement Program

The Citrix Customer Experience Improvement Program (CEIP) gives you the opportunity to contribute to the design and development of Citrix products. When you enroll in the program, Citrix collects anonymous information about your deployment, which is used to improve product quality, reliability, and performance.

It's easy to enroll in the program after you create or upgrade a Site. You can also opt in or out of the program at any time by selecting Configuration in the Studio navigation pane and following the instructions.

For more information, see About the Citrix Customer Experience Improvement Program.

Enhanced connection throttling settings

To improve performance, you can now specify the maximum number of simultaneous actions, simultaneous Personal

Storage inventory updates, and actions per minute that can occur on a host connection.

For more information, see Edit a connection.

Enhanced reporting in Studio

Studio displays more detailed status and error reporting when updating PvD images, and displays comprehensive licensing alerts when you are in the licensing node.

SSL/TLS

You can enable Secure Sockets Layer (SSL/TLS) connections between users and VDAs by configuring SSL/TLS on the machines where the VDAs are installed and in the Delivery Groups that contain the VDAs.

For more information, see SSL.

Virtual IP and virtual loopback

For published applications, you can enable and use the Microsoft virtual IP feature in machines running Windows Server 2008 R2 and Windows Server 2012 R2. Additionally, you can add new Citrix policy settings to manage virtual loopback. A preferred loopback option is also available.

For more information, see Virtual IP and virtual loopback.

Client and session clipboard write

You can restrict or enable sharing of data from the host clipboard to the client or from the client clipboard to the user session. In each case, when sharing is restricted, you can specify data formats that can be shared.

For more information, see ICA policy settings.

Remote PC Access

You can now prevent a local user from disconnecting a remote session without the permission of the remote user.

When disconnecting a remote session, moving the mouse or pressing a keyboard key wakes the local monitor. (In previous releases, pressing CTRL+ALT+DEL twice presented the logon screen.)

Icon locations are now preserved when connecting from a lower resolution device and then returning to a larger resolution device.

Generic USB Redirection

This release provides support for Generic USB Redirection for specialty USB devices for which there is no optimized virtual channel. This functionality redirects arbitrary USB devices from client machines to virtual desktops; with this feature, end users have the ability to interact with a wide selection of generic USB devices in the desktop session as if the devices were physically attached.

With Generic USB Redirection:

- users do not need to install device drivers on the user device
- USB client drivers are installed on the VDA machine

This feature requires Windows Server 2012 R2, and functions with existing Windows Receiver versions for published desktop

sessions hosted on RDS hosts in single-hop scenarios. Using this feature, USB client drivers are installed on the host, so these drivers must be compatible with RDSH for Windows 2012 R2 platforms.

Citrix Director 7.6.100

Director 7.6.100 includes the following new and enhanced features. For download, installation, and upgrade information, see http://support.citrix.com/article/CTX200330.

- **Virtual machine usage.** Provides administrators with the real-time view of their VM usage so they can quickly assess their site's capacity needs. VM usage is categorized by Desktop OS availability and Server OS availability.
  - **Desktop OS availability.** Displays the current state of Desktop OS machines (VDIs) by availability for the entire site or specific Delivery Group.
  - **Server OS availability.** Displays the current state of Server OS machines by availability for the entire site or specific Delivery Group.
- **Export improvements.** Enhanced to provide the option of exporting the trends reports in CSV, PDF, and Excel formats.
- **Zoom-in drilldown enhancements.** Drilldown capabilities were added to Director 7.6. This enhanced feature lets administrators navigate through trend charts by zooming in on a time period (clicking on a data point in the graph) and drilling down to see the details associated with the trend. The administrators can now better understand the details of who or what has been affected by the trends being displayed.

New features in Director 7.6

Licensing alerts making you aware of issues that may impact user connections. Director also displays a recommended action to correct the condition. Some of the conditions displayed in Director are:

- All licenses have expired.
- Licenses are about to expire.
- Citrix license grace period has expired.
- The Supplemental Grace Period is active, and all installed licenses are currently in use.

View hosted applications usage. You can select the Delivery Group and time period to view a graph displaying peak concurrent usage and a table displaying application-based usage. From the Application Based Usage table, you can choose a specific application to see details and a list of users who are using or have used the application.

Monitor hotfixes. You can view the hotfixes installed on a specific machine VDA (physical or VM) using the User Details or Machine Details view.

The filtering feature has been expanded. Filter data is clickable and leads to User Details, Machine Details, Endpoint Details, and Anonymous Sessions.

Director is compatible with XenApp 6.5. You can use Director to monitor your XenApp 6.5 deployments.

For information, see Director.

AppDNA 7.6

Citrix AppDNA accelerates the migration and transformation of desktop and web applications for new environments through rapid analysis, automated application remediation and packaging, and daily application management. AppDNA 7.6 includes a new Build Assessment solution that tests whether applications will work on additional builds of the same OS family. AppDNA 7.6 analysis enhancements now indicate whether required applications, application frameworks, and files are present, whether enabled GPOs will cause issues, and whether web applications are compatible with Citrix WorxWeb.

For information, see AppDNA 7.6.

Citrix StoreFront 2.6

Simplified store configuration in the administration console. The updated StoreFront console simplifies the StoreFront configuration for the following features:

- User subscriptions
- Set session timeout for Receiver for Web
- Show domains list in logon page

Receiver for Web My Apps Folder View. This new view displays the applications in a folder hierarchy and includes a breadcrumb path for unauthenticated and mandatory stores. This folder view can help your users move from Web Interface to Receiver for Web.

Kerberos constrained delegation for XenApp 6.5. StoreFront with Kerberos constrained delegation enables pass-through authentication, eliminating the need for the client and device to run Windows with Receiver.

Single Fully Qualified Domain Name (FQDN) access. With this feature, you can provide access to resources internally and externally using a single FQDN.

XenApp Services Support smart card authentication. The StoreFront server authenticates using smart cards to XenApp Services Support sites and does not require specific versions of Receiver and operating systems.

Receiver for Android, iOS, and Linux smart card authentication. New versions of Receiver support local and remote use of smart cards for accessing apps and desktops.

Extensible authentication. Support for extensible authentication provides a single customization point for extension of StoreFront's form-based authentication. Worx Home and Receiver for Web use it to authenticate with XenMobile and XenApp and XenDesktop for both internal (direct) and external (using NetScaler Gateway) access scenarios.

For information, see StoreFront 2.6.

Support for Citrix Connector 7.5

Citrix Connector 7.5 provides a bridge between Microsoft System Center Configuration Manager and XenApp or XenDesktop, enabling you to extend the use of Configuration Manager to your Citrix environments. Citrix Connector 7.5 support now includes the Platinum editions of XenApp 7.6 and XenDesktop 7.6.

For information, see Citrix Connector 7.5 for System Center Configuration Manager 2012.

Support for Receiver for Chrome 1.4 and Receiver for HTML5 1.4

Receiver for Chrome enables users to access virtual desktops and hosted applications from devices running the Google Chrome operating system. Users access these resources through Receiver for Chrome, and their desktops and applications are displayed in a single window.

Receiver for HTML5 is hosted on StoreFront servers and enables users to access virtual desktops and hosted applications from a web browser. Users can access desktops and applications within their web browsers without needing to install Citrix Receiver on their devices.

In this release, both these Receivers include the ability to convert documents to PDF from hosted applications or applications running on virtual desktops and view them on a local device or print to a locally attached printer; enhanced

clipboard operations; end-user experience metrics; and the ability to track licence usage for hosted applications.

For information, see Receiver for Chrome 1.4 and Receiver for HTML5 1.4.

Support for HDX Real-Time Optimization Pack 1.5 for Microsoft Lync

HDX Real-Time Optimization Pack 1.5 for Microsoft Lync supports Lync-certified USB phones, mixed Lync 2010 client and Lync Server 2013 configuration, and asynchronous upgrades.

For information, see HDX Real-Time Optimization Pack 1.5 for Microsoft Lync.

Feature Pack 3: Install and upgrade

Feb 24, 2016

This article gives short install instructions for all the components in XenApp and XenDesktop 7.6 FP3 - what to install and where. Check System requirements and product article links for detailed instructions.

Download the FP3 components from citrix.com. Availability depends on your current entitlement.

Workstation OS VDA 7.6.300

Download and run **VDAWorkstationSetup.exe** on the machine where you want install the VDA. Use either the graphical interface or the command line.

For more information, see Install VDAs using the standalone package.

To upgrade VDAs installed on machines running Windows 8.x or Window 7 to Windows 10, reimage Windows 7 and Windows 8.x machines to Windows 10 then install the supported VDA for Windows 10 using the standalone package.

For more information, see Upgrade a deployment.

Server OS VDA 7.6.300

Download and run **VDAServerSetup.exe** on the machine where you want install the VDA. Use either the graphical interface or the command line.

The VDA for Windows Server OS installation automatically deploys Microsoft Visual C++ 2013 runtime (32-bit and 64-bit), as well as 2008 and 2010 runtimes (32-bit and 64-bit). Microsoft Visual C++ 2005 is no longer deployed. These pre-requisites will initiate a server restart, with the VDA installation continuing after the restart.

For more information, see Install VDAs using the standalone package.

Group Policy Management 7.6.300

The new and enhanced HDX technologies features in this release are included in the Feature Pack 3 VDA and managed using the updated Group Policy Management package.

On the server where you manage Citrix policies, download and run **CitrixGroupPolicyManagement_x64.msi** or **CitrixGroupPolicyManagement_x86.msi**. Then launch Studio or GPMC and the new and updated policies are displayed.

For more information on the updated policies, see: Visual display policy settings for enhanced Thinwire compatibility mode; USB devices policy settings for support for signature devices and drawing tablets; Flash redirection and Multimedia policy settings for video fallback prevention; and Framehawk policy settings for the HDX Framehawk virtual channel.

Active Directory Deployment Tools 7.6

Contains scripts (**InstallVDA.bat** and **UninstallVDA.bat**) that install, upgrade, or remove Virtual Delivery Agents (VDAs) for groups of machines in Active Directory. Scripts must be modified before use.

For more information, see Install or remove Virtual Delivery Agent using scripts.

Universal Print Server 7.6.300

The UPS package contains updated versions of the standalone UPS server component (**UpsServer_x64.msi** and **UpsServer_x86.msi**) and prerequisites (**vcredist_x64.exe**, **vcredist_x86.exe**, **cdf_x64.msi** and **cdf_x86.msi**).

On a Windows Server 2012 R2 or Windows Server 2012 print server, install the UPServer component by extracting and then launching the component's MSI, UpsServer_x64.msi or UpsServer_x86.msi. A restart is required after installing the UPServer component.

The UPClient component, which you install on XenApp and XenDesktop hosts that provision session network printers is part of the VDA installation.

Additional steps are required for environments where you want to deploy the UPClient component separately, for example with XenApp 6.5.

For more information on all of these configurations in FP3, see Provision printers.

Additional steps are also required to deploy UpsServer_x86.msi on the Windows 2008 32-bit platform. For more information, see Install using the command line.

Director 7.6.300

Check that you have selected all the required features in IIS. For the full list, see CTX142260. Download and run **DesktopDirector.msi** on the server running Director. Install the CitrixGroupPolicyManagement.msi if you haven't already done so.

Use the WMIProxy MSI files included in the package to install or upgrade the WMIProxy on the VDA.

Use the XDPoshSnapin MSI included in the package to upgrade the XDPoshSnapin_Hotfix on the Delivery Controller. This is required for delegated administrators and custom administrators to view the Framehawk virtual channel information in Director.

For full install and configuration instructions, see Director.

AppDNA 7.6.5

AppDNA 7.6.5 includes new Windows 10 reports to help you understand whether your application from Windows XP or later will run on Windows 10. Download the installer, **Citrix-AppDNA.msi**, and run it in a VM. The installer handles first time and upgrade installations for all licensing types. For trial licenses, the installer creates a database that will work with Microsoft SQL Server Express.

For more information, see Install AppDNA.

StoreFront 3.0.1

To install, download and run **CitrixStoreFront-x64.exe** as an Administrator on the StoreFront server. StoreFront 3.0.1 includes Citrix Receiver for HTML5 1.8.

For more information, see Install, set up, and uninstall.

To upgrade, disable access to the StoreFront deployment and restart the StoreFront server. Download and run **CitrixStoreFront-x64.exe** as an Administrator on the StoreFront server(s).

For more information, see Upgrade.

Citrix Receiver for HTML5 1.8

Receiver for HTML5 is hosted on StoreFront and a version of Receiver for HTML5 comes by default with StoreFront. StoreFront 3.0.1 includes Citrix Receiver for HTML5 1.8. If you are running an earlier version of StoreFront and want to install or upgrade to this version of Citrix Receiver for HTML5, you can download and run Receiver for HTML5 1.8 (**CitrixHTML5Client-x64.exe**) on StoreFront 2.5 or higher.

For more information, see Configuring Citrix Receiver for HTML5.

Citrix Receiver for Windows 4.3.100

Receiver for Windows 4.3.100 is included in the VDA 7.6.300 packages delivered with FP3. Use the Citrix Receiver for Windows 4.3.100 (CitrixReceiver.exe) for upgrading Receiver on earlier VDAs or for installing or upgrading on user devices.

If the Citrix Lync Optimization Pack is installed on the endpoint device it must be uninstalled first and then reinstalled after upgrading Citrix Receiver for Windows. See CTX200340.

For more information, see Install.

Linux Virtual Desktop 1.1

Prepare your Linux virtual machines, install the new Linux VDA software on them, configure your Delivery Controller, and then use Studio to make the desktops available to users.

For more information, see the Linux Virtual Desktop Installation Guide for SUSE and the Linux Virtual Desktop Installation Guide for Red Hat.

XenServer 6.5 SP1 hotfix for Windows 10 certified drivers

This is a hotfix for customers running XenServer 6.5.0 Service Pack 1. This hotfix provides Windows 10 certification for the standard Windows drivers.

For more information, see CTX201974.

Feature Pack 3: Fixed issues

Mar 01, 2016

Citrix Director 7.6.300; 7.6 LTSR

- The Activity Manager in Director might fail to show the applications that are open for some users.
  [#LC2325]
- Director site names are truncated when there are multiple sites configured.
  [#LC2967]

Citrix Universal Print Server 7.6.300; 7.6 LTSR

Universal Print Client

Universal Print Server

Universal Print Client Issues

- The print preview might be slow in showing the Office documents while using network printers.

  [#LC1205]
- On servers with XenApp 6.5 Hotfix Rollup Pack 4 and Universal Print Client 7.6 installed, the session on the user device might become unresponsive.

  [#LC1562]
- This feature enhancement implements performance counters for the Universal Print Server and Universal Print Client.

  [#LC1820]
- When attempting to print from Adobe Reader X1, the print dialog can take up to twenty seconds to appear.

  [#LC2412]
- Occasionally, the Citrix Print Manager service (cpsvc.exe) might unexpectedly stop running when users log on to a VDA.

  [#LC2716]
- When the Universal Print Server is installed on a VDA but disabled by Citrix policies, PowerShell get-printer commands on the VDA might fail.

  [#LC2966]
- Intermittently, the print spooler service can experience a fatal exception on UpProv.dll.

  [#LC3055]

Universal Print Server Issues

- This fix addresses a memory issue in an underlying component.

[#LC1381]

- This feature enhancement implements performance counters for the Universal Print Server and Universal Print Client.

  [#LC1820]

- This fix addresses a memory issue in an underlying component.

  [#LC2764]

VDA for Desktop OS 7.6.300; 7.6 LTSR; 7.7

The versions of the VDA for Desktop OS included in XenApp and XenDesktop 7.6 Feature Pack 3 (7.6.300) and 7.6 LTSR are identical. The version included in XenApp and XenDesktop 7.7 contains the same fixes as Version 7.6.300, plus compatibility updates for XenApp and XenDesktop 7.7.

Broker Agent

- VDAs can becomes stuck in the initializing state of the registration process. The issue occurs after the Citrix Desktop Service runs for several days without being restarted.

  [#LC0570]

- When the function "CName" is enabled, VDA registration can take excessively long. With this fix, turning on the "CNameSuppressOrgFqdnLookup" value speeds up the registration process.
  Important: You must enable "CName" if you enable "CNameSuppressOrgFqdnLookup."

  To enable the fix, you must create the following registry key:

  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent

Name: UseCnameLookup
Type: REG_DWORD
Value: Enabled = 1 (Disabled=0)

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
  Name: CNameSuppressOrgFqdnLookup
  Type: REG_DWORD
  Value: Enabled = 1 (Disabled=0)

[#LC0791]

- Attempts to reconnect to a VDA through a user session might fail if the VDI-in-a-Box mode is enabled.

  [#LC1522]

- If a Version 7.6 VDA is a member of a XenDesktop 5.6 site, when users connect, disconnect, and then try to connect again, the reconnection attempt fails and the VDA is unregistered.

  [#LC1859]

HDX 3D Pro

- When users load a customized cursor in a HDX 3D Pro desktop, the correct cursor color does not appear.

  [#LC0917]

- When moving the mouse cursor over the toolbox bar and drawing area of a third-party CAD application in which the desktops are HDX 3D Pro-enabled and running Windows with Simplified Chinese, the mouse cursor might disappear.

  [#LC1321]

- After disconnecting the Citrix Receiver session, reconnecting to a locked VDA session can fail on a computer with HDX 3D Pro with NVIDIA graphics card.

  [#LC1629]

- In dual-monitor HDX 3D Pro VDA sessions that are calibrated to to 150% DPI, the mouse pointer and other screen art-effects can appear outside the VDA session and thus be inaccessible.

  [#LC2502]

- When hardware acceleration is enabled, AutoCAD 2011 fails in a Receiver session after resizing the CD Viewer window.

  [#LC2531]

- With this fix, the bandwidth cap for HDX network traffic is 20 megabits per second (Mbps).

  [#LC2780]

- Graphics can appear blurred in VDA sessions in HDX 3D Pro environments with an NVidia Grid K1 graphics board and if the VDA is connected to a high latency WAN network.

  [#LC2877]

- On VDAs with HDX 3D Pro enabled, the lossless indicator taskbar icon (for LLIndicator.exe) might fail to indicate the lossless state and might not respond when right-clicked.

[#LC2931]

- The mouse cursor might disappear after the user locks or unlocks a session for a few times on an HDX 3D Pro desktop.

  [#LC3188]

- When the Desktop Viewer switches from full-screen mode to window mode, the HDX 3D Pro session might become unresponsive for a few minutes.

  [#LC3193]

- HDX 3D Pro might unexpectedly start on the VDA even though has not been installed. This can occur when Windows XP display driver model (XPDM) is installed on the VDA instead of Windows display driver model (WDDM).

  [#LC3215]

HDX MediaStream Flash Redirection

- When using Microsoft Internet Explorer 9 and later versions of the browser, if you click a link to a Flash redirected video while another Flash redirected video is already playing, the audio streams of the two videos overlap.

  This fix does not eliminate the issue, but setting the following registry key on the server allows you to shorten the amount of time during which it occurs:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  Name: UrlListForTerminationFlashInst
  Type: REG_MULTI_SZ
  Data: <URLs of affected websites; include both http:// and https://, each on a separate line; for example:
  http://www.youtube.com/; https://www.youtube.com/>

  [#LC0453]

- When using Microsoft Internet Explorer 9 or later, Flash redirection can fail for videos embedded in websites. A black rectangle appears in place of the video.

  To enable this fix, you must set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  Name: WorkWithAeroEnabled
  Type: REG_DWORD
  Data: 0

  [#LC0477]

- After using YouTube's built-in Search field In Microsoft Internet Explorer 8 and later versions of the browser, HDX Flash Redirection reverts to server-side rendering.

  To enable this fix, you must set the following registry key on the server:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  Name: SupportedUrlHeads
  Type: REG_MULTI_SZ
  Data: <each value on a separate line, null separated>
  http://

https://
file://

Note: SupportedUrlHeads was first introduced in Fix #LA4151. It is also used by this fix. If you add SupportedUrlHeads to the Registry, Flash Redirection ignores a Flash instantiation request unless the targeted URL starts with one of the headers specified in SupportedUrlHeads.

[#LC0505]

- Flash redirection fails for videos embedded on cnn.com and msn.com. A black rectangle appears in place of the video.

  In order to enable this fix, you must set the following registry keys:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ASJSCallbacks

  For cnn.com:

  Name: cnn.com
  Type: REG_MULTI_SZ

Data:	javaScriptLoaded
	setQueueAutoplay
	setAdVisibility
	setPlayerMode
	setAdSection
	setAdKeyValue
	playContent
	getContentEntry
	switchTrackingContext

  For msn.com:

  Name: msn.com
  Type: REG_MULTI_SZ

Data:	MsnVideoCallback
	MsnVideoPropertyCallback

GetWidgetID

Note: This fix works only for Internet Explorer 9 and later.

[#LC0665]

- When using Microsoft Internet Explorer 10, Flash redirection can fail for videos embedded in cnn.com websites. This occurs when the first video on the website is automatically played. Some contents in the page from this video, such as title, status, and advertisement, might be missing.

  [#LC0830]

- Flash redirection fails for videos embedded on m.mlb.com and msn.com. A black rectangle appears in place of the video.

  To enable this fix, set the following registry keys:

  For mlb.com:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ASJSCallbacks
  Name: m.mlb.com
  Type: REG_MULTI_SZ
  Data: <place each value on a separate line, null separated>
  setPlaylist
  startPlaylist

  For msn.com:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ASJSCallbacks
  Name: msn.com
  Type: REG_MULTI_SZ
  Data:<place each value on a separate line, null separated>
  MsnVideoCallback
  MsnVideoPropertyCallback
  GetWidgetID

  This fix works only for Internet Explorer 9 and later. To allow this to work, set Internet Explorer to run in emulation mode and set Internet Explorer versions 9 and 10 to document mode. For more information, see article CTX136588 on the Citrix Support site.

  [#LC1043]

- Internet Explorer might close unexpectedly when attempting to play a video in web sites where:

  - The option "Disable Flash acceleration" is enabled or if the site is blacklisted.
  - The user is using a Receiver version that does not support Flash redirection such as Receivers for Mac OS X, iPad, iPhone, and Android.

  [#LC2256]

HDX MediaStream Windows Media Redirection

- This release fixes redundant frames generated by the HDX graphics encoder, resulting in a smoother frame-rate and better

interactivity.

[#LC2177]

- When playing a video file in a VDA session with Receiver for Windows version 13.3 or 13.4, synchronization occurs between the audio and video in a custom application. However, when upgrading to a newer version of Receiver, Windows Media Redirection fails. After this occurs, users can hear audio only or can see video only.

  To enable this fix, you must use Citrix Receiver for Windows 4.3.

  [#LC2516]

- Attempts to close Windows Media Player with a video that is paused can cause Windows Media Player to become unresponsive.

  [#LC0728, #LC3410]

Installing, Uninstalling, Upgrading

- Earlier updates to the VDA for Desktop OS attempt to install a WDDM driver. In scenarios where you used the /nocitrixwddm switch during the original installation of the VDA to suppress the installation of the WDDM driver, installing an update causes the installation process to go into a loop that has the VDA restarting continually. With this fix, no attempt is made to install the driver when you update a VDA where the installation of the driver was suppressed originally.

  [#LC0443]

- Installing any VDA hotfix that was released before ICAWS750WX64012 reverts the state of the Citrix Remote Multi-Touch Device and Citrix Multi-Touch Redirection Services to the defaults, regardless of whether you manually enabled or disabled them previously.

  [#LC0446]

- Installing hotfixes for XenApp 7.5, and XenDesktop 7.1 and 7.5 VDA Core Services for Windows Desktop and Server OS released before September 2014 causes the ICA Session performance monitor counter to be removed. This can have an adverse effect on the operation of tools and processes that rely on these counters. This fix restores counters removed in this manner by the installation of earlier hotfixes and prevents their removal when installing subsequent hotfixes.

  [#LC0771]

- The VDA might fail to register after downgrading VDAs from version 7.6 to 5.6.400.

  [#LC1465]

- After upgrading VDAs, the following issues occur:

  - The registry entry EnableReadImageFileExecOptionsExclusionList changes to "outlook.exe."
  - Outlook cannot work with a smart card.

  This fix removes "outlook.exe" from the registry EnableReadImageFileExecOptionsExclusionList. Any other strings in this registry entry remain.

  [#LC1655]

- When users upgrade a VDA to version 5.6.400 or 5.6.500 and then copies files from a mapped client drive to the VDA or opens the files directly from the drive, the following error message appears:

"The Handle is Invalid."

[#LC1910]

- Attempts to restart the Print Manager Service by using the Services snap-in fail. The error message "Couldn't stop this service" appears and the status of the Print Manager Service shows "stopping."

  [#LC2122]

- After upgrading VDAs from XenDesktop 7.5 to XenDesktop 7.6, when users attempt to connect, error 1030 appears. In the System Event log shows the following message: "The Citrix ICA Transport Driver received an invalid Transport packet on port 2598."

  [#LC2501]

- Earlier updates to the VDA for Desktop OS attempt to install a WDDM driver. In scenarios where you used the /nocitrixwddm switch during the original installation of the VDA to suppress the installation of the WDDM driver, installing an update causes the installation process to go into a loop that has the VDA restarting continually. With this fix, no attempt is made to install the driver when you update a VDA where the installation of the driver was suppressed originally.

  [#LC3052]

- In rare cases, installing or reinstalling the MSP hotfix package can cause the Citrix Display Driver (Citrix Systems – WDDM) to be marked for deletion. This causes the installation to fail, which leaves the VDA's display resolution unusable.

  [#LC3312]

Keyboard/Mouse

- Automatic keyboard display might not function when using OpenOffice applications on an iPad device.

  [#LC2717]

Local App Access

- In a full screen mode desktop session, when Local App Access is enabled and the setting "Show windows contents while dragging" is disabled, high resolution pictures become distorted when moving application icons over the pictures in Internet Explorer.

  [#LC1722]

Logon/Authentication

- The error message "No valid certificates found" appears when users attempt to start an application through StoreFront with smart card authentication. This prevents users from logging on.

  [#LC1704]

Printing

- The Citrix Print Manager Service (CpSvc.exe) process might exit unexpectedly.

  [#LA5682, #LC1770]

- "Session printers" policies that are set without adding network printers can block the creation of session printers specified in

other "Session printers" policies.

[#LC0705]

- After changing the default printer in a VDA, when restarting the VDA and if users did not log off from the ICA session, the previous default printer appears in the VDA.

  [#LC0898]

- This fix reinstates the "Legacy printer names" policy, which was not previously available in Version 7.x of the product.

  [#LC1002]

- The Citrix Print Manager Service (CpSvc.exe) process might exit unexpectedly if the value for "pServerName" is incorrect.

  [#LC1241]

- When the "Auto-Create Generic Universal Printer" policy setting is enabled, the Citrix Print Manager Service (CpSvc.exe) does not create the Citrix Universal Printer generic printer.

  [#LC1255]

- This feature enhancement implements performance counters for the Universal Print Server and Universal Print Client.

  [#LC1820]

- The first page might be printed blank when using the Citrix Universal Print Driver.

  [#LC2771]

- The "Universal printing EMF processing" policy remains set to the default value even if you set it to "Reprocess EMFs for printer."

  [#LC2521]

- Users might experience intermittent delays when attempting to print documents or select a different printer, seeing the message "Connecting to printer" for up to a minute.

  [#LC2701]

- After applying Fix #LC0898 and configuring Session Roaming, creating printers in client printers and session printers fail.

  [#LC3490]

Remote PC

- If users start a Receiver session when there are existing Remote Desktop and console sessions to the same RemotePC VDA, the Receiver session fails with the message "Reconnecting...." This message appears indefinitely until users manually close the Receiver session.

  [#LC0627]

- If you log on to a physical Remote PC console within roughly 30 seconds of being presented with the logon screen after restart, you cannot establish a Remote PC ICA session to that VDA for the duration of the original session.

  [#LC3603]

Seamless Windows

- Maximized seamless applications do not resize correctly when moving a docked application, such as the Windows taskbar.

  [#LC1342]

- The seamless window does not appear even though the application process is running and the session exists on the server VDA.

  [#LC1728]

Session/Connection

- When reconnecting to a VDA session using a different connection method than for the initial session (for example, with and without using the Access/NetScaler Gateway), Citrix policies are not reevaluated for the reconnected session.

  Note: This fix requires you to delete all entries in the following locations on the Windows Desktop OS or Windows Server OS device. Do not apply this fix unless you are affected by the issue as described:

  - Registry : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix
  - Folder: C:\ProgramData\Citrix\GroupPolicy*.*

  [#LA5051]

- In scenarios with two dual-monitor endpoints A and B with identical screen resolutions, when you disconnect from endpoint A and then reconnect from endpoint B, all top-level windows are repositioned to the primary monitor.

  [#LA5440]

- Opening a published application and then running the explorer.exe command to open Windows Explorer can cause the desktop to open instead of Windows Explorer.

  Note: After installing this fix, the explorer.exe process might exit unexpectedly. For more information, see Knowledge Center article CTX128009.

  [#LC0285]

- When reconnecting to a Receiver session, the CPU consumption can be high if many Windows Explorer instances are running on a VDA. Additionally, minimized windows get maximized intermittently before getting minimized into the Windows taskbar again.

  [#LC0315]

- When connecting a USB magnetic card reader device, the device is recognized in the virtual desktop but the correct drivers do not load.

  [#LC0360]

- When you press the Windows+Left/Right arrow keys to move an application to the edge of the screen, then disconnect and reconnect to the session, the application is resized. The degree of the resizing varies by application and is greater on non-primary monitors.

  [#LC0386]

- Occasionally, user sessions might become unresponsive and can fail to log off. This also occurs if users log off manually from the console.

[#$LC0472]

- If the setting "Simplify device connections" is disabled in a USB redirection policy, SafeNet UKey USB devices might not work.

  [#LC0480]

- When users close a published version of Visual Basic Editor from the taskbar, open published Excel spreadsheets also close.

  [#LC0534]

- If an SD card is inserted into the user device and then a VDA session starts, if the card is redirected by client drive mapping it appears as a floppy disk in Windows Explorer.

  To enable the fix, set the following registry keys:

  - On 32-bit systems:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\UNCLinks
    Name: DisableFLoppyIcon
    Type: REG_DWORD
    Value: 1
  - On 64-bit systems:
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\UNCLinks
    Name: DisableFLoppyIcon
    Type: REG_DWORD
    Value: 1

  [#LC0616]

- On the user device, attempts to remote the combo box control under Region and Language > Date and Time formats might fail. This can occur when the combo box control has been successfully remoted once and a second attempt is made to remote it.

  [#LC0836]

- Redirected COM port devices might fail to work in a Receiver session.

  [#LC0851]

- A "Connection Established, Negotiating Capabilities" pop-up window appears from the Receiver when the VDA becomes unresponsive. To start any other sessions successfully, restart the VDA.

  [#LC0909]

- The time zone is not correct when users log on with Receiver for Windows. For this hotfix to work correctly, you must install the following:

  - The same Microsoft time zone update hotfix on the user device and the server. For example, if Microsoft Hotfix KB2998527 is installed on the user device, install this hotfix on the server.
  - Microsoft Hotfix KB2870165 on the server if the server operating system is Windows Server 2008 R2 Service Pack 1.
  - Fix #LC1392 is installed on the user device.

  [#LC1061]

- If the USB redirection policy contains more than 1000 characters all USB drives are redirected, even if there is a deny rule for the device.

[#LC1153]

- When ExcelHook is enabled and multiple projects are opened in Microsoft Project 2013, the first project opened might not appear in the taskbar.

  [#LC1158]

- When Desktop Composition Redirection (DCR) is used on wide area network (WAN) connections, web pages or documents that show text and graphic content might become unresponsive and can also consume high bandwidth.

  [#LC1256]

- The final image quality might degrade if the settings "Build to lossless" and "Allow Visually Lossless Compression" are enabled on the Desktop Delivery Controller (DDC).

  [#LC1271]

- When users log on for the first time, the screen might appear corrupted in the Receiver session. The issue occurs when you change Visual quality to "Build to lossless" and enable the "Allow visually lossless compression" setting.

  [#LC1272]

- When a two-monitor setup is used for a server VDA session, attaching or detaching the secondary monitor might cause the primary monitor to become unresponsive.

  [#LC1359]

- When users attempt to connect to a disconnected session, it can take up to three minutes to establish the connection.

  [#LC1376]

- Users cannot switch from a Remote Desktop (RDP) session to a Receiver session.

  [#LC1383]

- Redirection might not work correctly for the MailTo feature in XenDesktop and XenApp sessions. When the user clicks on the "MailTo" link in the web browser, instead of opening the published Microsoft Outlook, an error appears.

  [#LC1400]

- When launching published applications, the Citrix Graphics (CtxGfx.exe) process can cause CPU consumption to be higher than normal.

  [#LC1404]

- When Session Lingering is enabled and an application is closed on an iOS or Android device, a black window appears and stays on the device screen.

  [#LC1407]

- When a USB storage device on a user device is connected to XenDesktop 5.6, if the registry value of "UNCEnabled" is set to "0" and the registry value of "InitialClientDriveLetter" is set to "N," the drive letter of the USB disk in a session starts from the default "V" instead of "N".

  For more information, see Knowledge Center articles CTX127968 and CTX122061.

[#LC1451]

- When users log off from a desktop session, WFShellWindow stops responding and the message "Wfshell needs to close" appears for three minutes.

  [#LC1591]

- Information remains visible on the screen after the VDA goes into screen saver or power save mode, until the user provides input (mouse or keyboard) which updates the session with a blank screen. This occurs when screen savers and the power-save option in sessions are enabled by the DWORD value HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\SetDisplayRequiredMode = 0.

  [#LC1650]

- A third-party application might become unresponsive in a XenDesktop session when accessing a mapped dongle.

  [#LC1657]

- If the UxPersistence key is enabled in the registry, attempts to move applications to the edge of the screen by using the Windows key and the left or right arrow keys fail after disconnecting and then reconnecting to a session.

  [#LC1684]

- When switching a Receiver connection to a Remote Desktop (RDP) session for a VDI, if the user answers "No" in the transfer logon dialog box for the RDP connection, reconnecting with Receiver fails with a status 1030.

  [#LC1696]

- When users log off from XenDesktop, in XenCenter or the vSphere console, the user desktop session appears for several seconds.

  [#LC1782]

- When users logon and then logoff with a smart card and then logs on with a user name and password, the connection starts and then disconnects almost immediately. This continues until the user connects with the smart card again.

  [#LC1831]

- If the keyboard layout of the user device is different from the keyboard layout of the VDA, the display might become unresponsive for about 60 to 70 seconds while starting a virtual desktop session from Receiver for Windows.

  [#LC1939]

- The CPU consumption of the WMI Provider Service can be higher in Windows server and desktop VDA and causes the VDAs to become unresponsive. Also, the Receiver connection fails.

  [#LC2041]

- Session screen resolution might fail to resize when users disconnected from a session using Citrix Receiver for Windows and reconnect to the same session, on a device with a smaller screen resolution, using Citrix Receiver for Linux or Citrix Receiver for Windows CE. This can occur when the "Legacy graphics mode" policy setting is enabled for the session.

  [#LC2079]

- If Lotus Notes is started on an iPad with Receiver for iOS, the application might close unexpectedly.

[#LC2124]

- In a XenDesktop session, a message box appears that says a service wants to show a message. When the user clicks "View the message," the XenDesktop session shows a black screen. The issue occurs when the XenDesktop VDA is already using session 0.

  [#LC2160]

- If legacy graphics are enabled, mouse pointer shadowing is not automatically disabled.

  [#LC2222]

- When users disconnect from a session, Citrix WinFrame Shell (WFShell.exe) causes high CPU utilization.

  [#LC2235]

- If users log on to the Web Interface from within a VDA desktop session and attempt to start the same desktop, the session might disconnect and the VDA becomes unresponsive. As a result, users might not be able to start the desktop and the VDA must be restarted.

  [#LC2267]

- If the default Unicode input language of the user device is different from the input language of the VDA, the session might become unresponsive while the session desktop is loading.

  [#LC2287]

- When opening a published application file from a Client Drive Mapping (CDM) and then saving the file after entering text, the modified time stamp does not update.

  [#LC2305]

- Wfshell.exe continues to use a large amount of CPU resources after users disconnect from a session.

  [#LC2391]

- With USB redirection enabled, attempts to use a Wacom tablet along with its pen fail.

  [#LC2409]

- If the keyboard layout of the user device is different from the keyboard layout of the VDA, the session might become unresponsive while the session desktop is loading.

  [#LC2466]

- After disconnecting from Receiver, connection attempts fail with Remote Desktop (RDP) when RDP 8 is enabled and Network Level Authentication (NLA) is not used.

  [#LC2480]

- When users connect by using single sign-on to StoreFront through NetScaler Gateway where ICA proxy is enabled and then log off and log on again, VDA policies do not work. When users disconnect and then reconnect, the policies work.

  [#LC2577]

- When Excelhook is enabled, switching between open Excel workbooks can lose the focus on the selected workbook.

Additionally, users cannot select any of the open Excel workbooks and the focus stays on the last chosen file.

#LC2589]

- Users cannot start applications after updating cipher registry keys. To apply this fix, install the new version of the SSL SDK.

  [#LC2729]

- When users reconnect to a VDA, if "User Experience Persistence" is enabled, application windows can be in an incorrect state, such as maximized instead of restored.

  [#LC2769]

- When a point-of-sales device is redirected to a shared desktop through the COM port, the device might not be recognized by third-party software running on the shared desktop.

  [#LC2775]

- When opening a published version of Internet Explorer on Windows Phone 8.1, if the device is turned horizontally, half of the screen appears as a blank window. Additionally, users cannot maximize the Internet Explorer window. If users turn the device vertically, the screen appears normal.

  [#LC2786]

- Microsoft Office applications might close unexpectedly while running on a VDA for Windows-based Desktop OS.

  [#LC2878]

- When using an external monitor along with a laptop, a white square can be visible in a corner of the external monitor. The issue arises specifically when the external monitor has a screen resolution different from the resolution of the primary monitor, is located to the left of the primary monitor, and its top edge is above the top edge of the primary monitor.

  [#LC3186]

- Microsoft Office applications might occasionally stop running unexpectedly, due to interactions with Citrix API hooks.

  [#LC3280]

- With USB Redirection disabled, disconnecting from a published application can cause the following, spurious Event 261 to appear in the Event Viewer:

  "The Citrix Device Redirector service could not complete an IO operation with the Redirector Bus."

  [#LC3439]

Site/Farm Administration

- Custom administrators that have all permissions cannot remove an offline server from the farm and receive an access denied error message when running the PowerShell command, "Remove-XAServer".
- [#LC0752]
- Policy processing might take a long time if servers have access only to a Read-Only Domain Controller.

  [#LC0828]

- If you are using RES software to manage your deployment and have the Instant LogOff policy enabled, session information might fail to be updated to the Citrix Broker Service on the XenDesktop Controller when users log off sessions, causing the Controller to reflect inaccurate session status.

  [#LC1173]

- This fix allows creation of persistence registry settings for user devices.

  [#LC1827]

- If the latency is high, the Group Policy engine (CitrixCseEngine.exe) can cause delays during logon.

  To enable this fix, create the following registry keys:

  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy
    Name: GpoCacheEnabled
    Type: REG_DWORD
    Value: 1
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy
    Name: CacheGpoExpireInHours
    Type: REG_DWORD
    Value: 5 to 24

  [#LC1987]

Smart Cards

- After upgrading VDAs, Microsoft Outlook does not prompt for a personal identification number (PIN) when users attempt to log on with a smart card. Instead, the following error message appears:

  "Please insert a smart card."

  [#LC0556]

- After authenticating using Citrix Receiver for Linux while a smart card is present in the reader attached to the endpoint, the session can become unresponsive.

  [#LC0982]

- The ActivIdentity (accompkcs.exe) process might exit unexpectedly with an exception on scardhook64.dll. As a result, the websites that require a smart card might not function until the VDA is restarted.

  [#LC1056]

- With this enhancement, removing a smart card reader from an endpoint results in the same behavior as removing a smart card from an endpoint. As a result, with the VDA smart card policy configured to "Lock Workstation," removing the reader disconnects the session, effectively locking the VDA.

  To enable the fix, set the following registry keys:

  - HKEY_LOCAL_MACHINE\Software\Citrix\SmartCard
    Name: ReaderUnpluggedDetectEnable
    Type: REG_DWORD
    Value: Non-zero value
  - HKEY_LOCAL_MACHINE\Software\Citrix\SmartCard

Name: ReaderUnpluggedDetectPollingInterval
Type: REG_DWORD
Value: 5 to 60 seconds (default polling interval is 10 seconds)
[#LC1059]

- This fix extends the functionality introduced by Fix #LA1059 so that the fix also takes effect for connections to Version 7.5 VDAs made from Windows 8.1 endpoints.

  From the description of #LA1059:

  With this enhancement, removing a smart card reader from an endpoint results in the same behavior as removing a smart card from an endpoint. As a result, with the VDA smart card policy configured to "Lock Workstation," removing the reader disconnects the session, effectively locking the VDA.

  To enable the fix, set the following registry keys:

  - HKEY_LOCAL_MACHINE\Software\Citrix\SmartCard
    Name: ReaderUnpluggedDetectEnable
    Type: REG_DWORD
    Value: Non-zero value
  - HKEY_LOCAL_MACHINE\Software\Citrix\SmartCard
    Name: ReaderUnpluggedDetectPollingInterval
    Type: REG_DWORD
    Value: 5 to 60 seconds (default polling interval is 10 seconds)

  [#LC1713]

- The VDA servers experience an error on icardd.dll and a blue screen appears.

  [#LC2277]

- Attempts to reconnect to VDA session by using a smart card with a personal identification number (PIN) fail and one of the following error messages appear:

  - Insert a smart card
  - Reading Card.

  If users log on by using a user name and password, the session connects.

  [#LC2596]

System Exceptions

- The operating system experiences an error on picadm.sys and a blue screen appears with bugcheck code 0x22.

  [#LC0227]

- Playing a video in a media player in a pass-through session can cause the session to exit unexpectedly.

  [#LC0553]

- The published version of Microsoft Excel 2010 fails when moving between open spreadsheet files.

  [#LC0809]

- The VDA experiences an error on ctxdvcs.sys with bugcheck code E3 that appears on a blue screen.

[#LC0857]

- The VDA might become unresponsive if a VDA session is maximized when using graphic applications.

  [#LC0908]

- Windows Explorer might close unexpectedly in one of the following cases:

  - When selecting a large number of files whose names contain more than 260 characters, and then selecting the "Send to > Fax recipient" option.
  - When attempting to open third party applications.
  - When attempting to combine files by using Nitro PDF.

  [#LC0938]

- A page fault in the ICA WSK Transport Driver (tdwsk.sys) causes the VDA to fail with an error on a blue screen.

  [#LC1032]

- After downgrading VDAs from version 7.6 to 5.6.400, the operating system experiences an error on vd3dk.sys and a blue screen appears with the stop code 0x3B.

  [#LC1200]

- The operating system experiences an error on picadm.sys and a blue screen appears. The issue occurs when the value of "TrucationResource" becomes null.

  [#LC1430]

- Playing an audio file from Receiver for HTML5 where SSL is enabled in the ICA session can cause the VDA to experience a fatal exception. displaying a blue screen.

  [#LC1752]

- Occasionally, the VDA might unexpectedly shut down and then restart.

  {#LC1876}

- The operating system experiences an error on ctxdvc.sys and a blue screen appears with bugcheck code 3B.

  [#LC2119]

- The operating system experiences an error on tdica.sys and a blue screen appears with bugcheck code 44 [MULTIPLE_IRP_COMPLETE_REQUESTS].

  [#LC2171]

- Windows Server 2008 R2 and Windows Server 2012 R2 might experience a fatal exception when users connect with Receiver for Windows.

  [#LC2179]

- After upgrading from Version 5.6 Rollup 4 to Version 7.6, VDAs can become unresponsive during shutdown.

  [#LC2245]

- Servers might experience an error on icausbb.sys and with the message PNP_DETECTED_FATAL_ERROR appearing on a

blue screen.

[#LC2811]

- The wfshell.exe process might close unexpectedly and prevent new connections.

  [#LC3024]

- When reconnecting to a disconnected session, the Group Policy engine (CitrixCseEngine.exe) might close unexpectedly.

  [#LC3091]

- The VDA might become unresponsive if a VDA session is maximized when using graphic applications.

  [#LC3279]

- VDAs might experience a fatal exception on vdtw30.dll, displaying a blue screen.

  [#LC3354]

- VDAs might experience a fatal exception on vd3dk.sys, displaying a blue screen with stop code 0x50. This can occur when Java-based upgrade tools are configured to upgrade the VDA at startup.

  [#LC3372]

- The explorer.exe process can exit unexpectedly when you attempt to connect to a session.

  [#LC3411]

User Experience

- This fix addresses the following issues with the way applications are represented in the Receiver for Windows taskbar:
  - Individual applications can display the default Receiver icon instead of the application-specific icon.
  - When multiple applications are running in the same session, they can appear grouped under a single, default Receiver icon.

  [#LC0094]

- This fix addresses a usability issue with Desktop Composition Redirection with Receiver for Windows prior to Version 4.200 when used over LAN connections.

  [#LC1507]

User Interface

- Occasionally, window positions are not retained when users reconnect to a VDA and are using multiple monitors.

  [#LC2075]

- The "Automatic Keyboard display" might not appear when users open a published application from Receiver for Windows or mobile Receivers.

  [#LC2747]

Miscellaneous

- This fix introduces the /Verbose option to vdaredirector.exe which causes a message window to appear when vdaredirector.exe runs. Unless the /Verbose option is specified, no message window appears.

[#LC0338]

- After installing third party antivirus software on a Microsoft Windows 8 (32-bit version) VDA, Citrix Receiver sessions cannot be started.

  [#LC1636]

- Users cannot change the Lync status in the console session if any Hotfixes contain Fix# LA5736 or if any of the following Hotfixes are present on the VDA:

  - ICAWS750WX64007
  - ICAWS750WX64008
  - ICAWS750WX64012
  - XD710ICAWSWX64003

  The Lync status always shows as "Away."

  Important: After applying this hotfix, if NetScaler Gateway is part of the deployment, the Lync status continues to show as "Away" when users disconnect from the VDA session and then connect to a console session.

  [#LC1691]

- Users cannot change the Lync status in the console session if any Hotfixes contain Fix #LA5736 or if any of the following Hotfixes are present on the VDA:

  - ICAWS750WX64007
  - ICAWS750WX64008
  - ICAWS750WX64012
  - ICAWS750WX64028
  - XD710ICAWSWX64003

  The Lync status always shows as "Away."

  [#LC2479]

- This release includes support for the Framehawk Virtual Channel, a new ICA virtual channel that extends Citrix HDX technologies to improve user experience on broadband wireless connections where packet loss and latency are common issues. For more information, see What's new.

  [#LC2782]

- This is an enhancement in support of a specific 5-in-1 COM port device. It ensures that the ID card reader function of the device works properly in VDA sessions.

  [#LC0325]

- Attempts to start VM hosted apps might fail if users indirectly belong to a nested group that is set to limit visibility.

  [#LC3589]

VDA for Server OS 7.6.300; 7.6 LTSR; 7.7

The versions of the VDA for Server OS included in XenApp and XenDesktop 7.6 Feature Pack 3 (7.6.300) and 7.6 LTSR are identical. The version included in XenApp and XenDesktop 7.7 contains the same fixes as Version 7.6.300, plus compatibility updates for XenApp and XenDesktop 7.7.

Broker Agent

- VDAs can becomes stuck in the initializing state of the registration process. The issue occurs after the Citrix Desktop Service runs for several days without being restarted.

  [#LC0570]

- When the function "CName" is enabled, VDA registration can take excessively long. With this fix, turning on the "CNameSuppressOrgFqdnLookup" value speeds up the registration process.
  Important: You must enable "CName" if you enable "CNameSuppressOrgFqdnLookup."

  To enable the fix, you must create the following registry key:

  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
    Name: UseCnameLookup
    Type: REG_DWORD
    Value: Enabled = 1 (Disabled=0)
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
    Name: CNameSuppressOrgFqdnLookup
    Type: REG_DWORD
    Value: Enabled = 1 (Disabled=0)

  [#LC0791]

- Attempts to start a published application in a multihomed server might fail with the following error:

  "There is no Citrix XenApp server configured on the specified address."

  [#LC1686]

- If a Version 7.6 VDA is a member of a XenDesktop 5.6 site, when users connect, disconnect, and then try to connect again, the reconnection attempt fails and the VDA is unregistered.

  [#LC1859]

HDX 3D Pro

- With this fix, the bandwidth cap for HDX network traffic is 20 megabits per second (Mbps).

  [#LC2780]

HDX MediaStream Flash Redirection

- When using Microsoft Internet Explorer 9 and later versions of the browser, if you click a link to a Flash redirected video while another Flash redirected video is already playing, the audio streams of the two videos overlap.

  This fix does not eliminate the issue, but setting the following registry key on the server allows you to shorten the amount of time during which it occurs:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  Name: UrlListForTerminationFlashInst
  Type: REG_MULTI_SZ
  Data: <URLs of affected websites; include both http:// and https://, each on a separate line; for example:
  http://www.youtube.com/; https://www.youtube.com/>

  [#LC0453]

- After using YouTube's built-in Search field In Microsoft Internet Explorer 8 and later versions of the browser, HDX Flash Redirection reverts to server-side rendering.

  To enable this fix, you must set the following registry key on the server:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  Name: SupportedUrlHeads
  Type: REG_MULTI_SZ
  Data: <each value on a separate line, null separated>
  http://
  https://
  file://

  Note: SupportedUrlHeads was first introduced in Fix #LA4151. It is also used by this fix. If you add SupportedUrlHeads to the Registry, Flash Redirection ignores a Flash instantiation request unless the targeted URL starts with one of the headers specified in SupportedUrlHeads.

  [#LC0505]

- When using Microsoft Internet Explorer 10, Flash redirection can fail for videos embedded in cnn.com websites. This occurs when the first video on the website is automatically played. Some contents in the page from this video, such as title, status, and advertisement, might be missing.

  [#LC0830]

- Internet Explorer might close unexpectedly when attempting to play a video in web sites where:

- The option "Disable Flash acceleration" is enabled or if the site is blacklisted.
- The user is using a Receiver version that does not support Flash redirection such as Receivers for Mac OS X, iPad, iPhone, and Android.

[#LC2256]

HDX MediaStream Windows Media Redirection

- After installing Versions 4.1 or 4.1.2 of the Receiver for Windows and if HDX MediaStream Multimedia Acceleration is enabled, Windows Media Player loads the video but the video fails to progress beyond the first frame.

  [#LC1460]

- This release fixes redundant frames generated by the HDX graphics encoder, resulting in a smoother frame-rate and better interactivity.

  [#LC2177]

- When playing a video file in a VDA session with Receiver for Windows version 13.3 or 13.4, synchronization occurs between the audio and video in a custom application. However, when upgrading to a newer version of Receiver, Windows Media Redirection fails. After this occurs, users can hear audio only or can see video only.

  To enable this fix, you must use Citrix Receiver for Windows 4.3.

  [#LC2516]

- Attempts to close Windows Media Player with a video that is paused can cause Windows Media Player to become unresponsive.

  [#LC3410]

Installing, Uninstalling, Upgrading

- If you install any of Hotfix Rollup Packs 1 through 4 after installing the Universal Print Server client, session printer enumeration can take an excessive amount of time.

  [#LA5977]

- Installing hotfixes for XenApp 7.5, and XenDesktop 7.1 and 7.5 VDA Core Services for Windows Desktop and Server OS released before September 2014 causes the ICA Session performance monitor counter to be removed. This can have an adverse effect on the operation of tools and processes that rely on these counters. This fix restores counters removed in this manner by the installation of earlier hotfixes and prevents their removal when installing subsequent hotfixes.

  [#LC0771]

- After installing Hotfix XA650R04W2K8R2X64008, existing icons that worked correctly with earlier versions of XenApp might be reported as corrupt.

  [#LC1081]

- After installing a Hotfix or Hotfix Rollup Pack that includes Fix #LA5872, when users log on with Receiver, the Windows logon security notice does not disappear until after the user's published application starts.

  [#LC1215]

- After installing XA650W2K8R2X64R04, occasionally, Discovery fails and it can take multiple tries to run Discovery

successfully.

[#LC1369]

- After installing Hotfixes XA650W2K8R2X64R03, XA650W2K8R2X64R04, or XA650W2K8R2X64R05, the following issues might occur:
  - Event Viewer fails when the following registry entries use German binaries:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{c6d0a271-2e59-40cd-b451-9000a9f104f9}
    - MessageFileName: C:\Program Files (x86)\Citrix\System32\resource\de\RaveEventMessages.Dll
    - ResourceFileName: C:\Program Files (x86)\Citrix\System32\resource\de\RaveEventMessages.Dll
  - If the operating system uses the English language and the default user account is set to use the German language, the RAVE event viewer uses German instead of English.

  [#LC2130]

- After installing Hotfix Rollup Pack 5, the XTE service fails and drops user sessions.

  {#LC2180

- After upgrading VDAs from XenDesktop 7.5 to XenDesktop 7.6, when users attempt to connect, error 1030 appears. In the System Event log shows the following message: "The Citrix ICA Transport Driver received an invalid Transport packet on port 2598."

  [#LC2501]

- After installing XA650W2K8R2X64R05 on XML Brokers, the time it takes for the XML Service to authenticate users can increase. In environments where there is a heavy load, this increase can be long enough to cause the user session to the Web Interface to time out.

  [#LC2536]

Keyboard/Mouse

- Certain keys might not function properly in a session using the Receiver for Linux with the Czech keyboard layout. Incorrect mappings can occur for the following characters:
  - ď will be incorrectly mapped as Ď
  - ň will be incorrectly mapped as Ň
  - ť will be incorrectly mapped as Ť

  Note: After installing this fix, when opening an RDP session from within a Receiver for Linux session there can be intermittent issues with the Shift key. To prevent this issue, Citrix recommends that you install Microsoft article KB2592687 on the Windows server. Alternatively, see Knowledge Center article CTX110281 for a workaround.

  [#LA3968]

- When switching between local and published applications by using the mouse, the keyboard input might not work.

  [#LA5849]

- The mouse pointer might not honor the boundaries of the desktop.

  [#LC0383]

- Mouse input can be intermittently lost within the session.

  [#LC0632]

- If the "Automatic keyboard display" policy is configured to show the keyboard on the user device, the keyboard does not appear automatically in the published application.

  Note: To completely fix this issue, install Fix #LC3158 on the user device.

  [#LC2432]

- Automatic keyboard display might not function when using OpenOffice applications on an iPad device.

  [#LC2717]

Local App Access

- In a full screen mode desktop session, when Local App Access is enabled and the setting "Show windows contents while dragging" is disabled, high resolution pictures become distorted when moving application icons over the pictures in Internet Explorer.

  [#LC1722]

Logon/Authentication

- The error message "No valid certificates found" appears when users attempt to start an application through StoreFront with smart card authentication. This prevents users from logging on.

  [#LC1704]

Printing

- The Citrix Print Manager Service (CpSvc.exe) process might exit unexpectedly.

  [#LA4967, #LA5682, #LC0344, #LC0427, #LC0675, #LC0781, #LC1090, #LC1770]

- When roaming to a different user device, an incorrect printer might be set as the default session printer.

  [#LC0225]

- This fix addresses an issue that prevents the following printers from being mapped into Receiver for Linux user sessions:

  - Epson-LQ-1050
  - Epson PLQ-20

  To enable this fix, you must set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\PrintingSettings
  Name: AllowPrinterMappingByName
  Type: REG_DWORD
  Data: 1

  [#LC0389]

- Session printers might fail to map to a session when reconnecting to a disconnected lingering session and the published application is a specified window size.

[#LC0615]

- The Citrix Print Manager Service (CpSvc.exe) fails due to an access violation.

  [#LC0660]

- If "Session Linger" is enabled, redirected printers on user devices might not map when reconnecting to a session.

  [#LC0816]

- This fix reinstates the "Legacy printer names" policy, which was not previously available in Version 7.x of the product.

  [#LC1002]

- When users log on to a new session, the printer list does not appear. The printer list does appear when users reconnect to a disconnected session.

  [#LC1226]

- When the "Auto-Create Generic Universal Printer" policy setting is enabled, the Citrix Print Manager Service (CpSvc.exe) does not create the Citrix Universal Printer generic printer.

  [#LC1255]

- This feature enhancement implements performance counters for the Universal Print Server and Universal Print Client.

  [#LC1820]

- Attempts to restart the Print Manager Service by using the Services snap-in fail. The error message "Couldn't stop this service" appears and the status of the Print Manager Service shows "stopping."

  [#LC2122]

- The "Universal printing EMF processing" policy remains set to the default value even if you set it to "Reprocess EMFs for printer."

  [#LC2521]

- The Citrix Printer Manager Service (Cpsvc.exe) quits unexpectedly with an access violation error.

  [#LC2624]

- Users might experience intermittent delays when attempting to print documents or select a different printer, seeing the message "Connecting to printer" for up to a minute.

  [#LC2701]

- The first page might be printed blank when using the Citrix Universal Print Driver.

  [#LC2771]

- Users cannot print with a Diebold printer (Model P361) when logged on with Receiver.

  [#LC2908]

- This enhancement creates one auto restored printer per port number when users log on.

[#LC2943]

Seamless Windows

- Seamless published instances of Microsoft Excel can experience screen flicker. Keyboard focus can also be lost to applications running locally.

  After installing this fix, you must create the following registry key and then the following two values:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\XLMAIN

  Name: ClassName
  Type: REG_SZ
  Data: XLMAIN

  Name: Type
  Type: REG_DWORD
  Data: 0x00000808

  [#LC0401]

- Maximized seamless applications do not resize correctly when moving a docked application, such as the Windows taskbar.

  [#LC1342]

- Applications with elevated permissions and published in Citrix Studio cannot start in seamless mode.

  [#LC1537]

- In a seamless session, attempts to dock a seamless toolbar in a second monitor always results in docking on the primary monitor when the seamless flag for published toolbars is set to ON. For more information about the seamless flag, see Citrix article CTX101644.

  [#LC1599]

- The seamless window does not appear even though the application process is running and the session exists on the server VDA.

  [#LC1728]

- In a multi-monitor environment, if the user moves the seamless window to a secondary display and then change the resolution of the primary or secondary display, the seamless window might move to the primary display.

  [#LC1819]

Session/Connection

- When the user attempts to save a file to a user device through client drive mapping, the file saved to the mapped drive might not contain any data.

  [#LA3566]

- After copying a file to a mapped client drive, the remaining disk space on the mapped drive can be calculated and displayed incorrectly.

[#LA4799]

- Attempts to reconnect to a session can experience a logon delay of up to 60 seconds even with multiple WMI filters configured through GPOs.

  To disable the policy calculation during reconnect, you must set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Reconnect
  Name: DisableGPCalculation
  Type: REG_DWORD
  Data: 1

  [#LA4932]

- The ConnectTime might not be recalculated during reconnect. As a result the Session Creation Server Duration (SCSD) and Session Startup Duration (SSSD) values can be unexpectedly high for certain sessions in EdgeSight reports.

  To enable the fix, you must set the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\wfshell
  Name: DisableServerStartupEventForReconnect
  Type: REG_DWORD
  Value: 1

  [#LA5141]

- Attempts to play an audio file in Microsoft Outlook might fail when users connect with Receiver for Mac.

  [#LA5657]

- With Excelhook enabled, attempts to switch among workbooks can fail and Excel can appear to be unresponsive.

  [#LA5708]

- After restarting the XenApp server, attempts to connect to the license server might fail.

  To enable this fix, you must create the following registry key:

  - On 32-bit Windows:
    HKEY_LOCAL_MACHINE\Software\Citrix\Licensing
    Name: RA_retries
    Type: REG_DWORD
    Value: 1 (if the value is not present or less than 5, the default value is considered as 5)
  - On 64-bit Windows:
    HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Licensing
    Name: RA_retries
    Type: REG_DWORD
    Value: 1 (if the value is not present or less than 5, the default value is considered as 5)

  [#LA5773]

- Attempts to reconnect to a locked published desktop session can fail with the following error message:

  "Connection Error: The Citrix server has reached its concurrent application limit for this application. Please contact your System Administrator."

When this occurs, a new session starts in addition to the existing session.

[#LC0158]

- Attempts to reconnect to a disconnected session can fail and a new session starts instead of the original session. The issue occurs when the "Restrict Remote Desktop Services users to a single remote session" setting is enabled.

  [#LC0201]

- When establishing a Remote Desktop (RDP) connection to a VDA and then disconnecting from the RDP session, the following error message (Event ID 1048) appears in the event log:

  "The Citrix Desktop Service is re-registering with the DDC:
  "NotificationManager:NotificationServiceThread: WCF failure or rejection by broker (DDC: bruin.newer.ln)""

  [#LC0251]

- With the application instance limit set to "1," attempts to restart an application from a disconnected session can fail and a new session might start. This is caused by an Automatic Client Reconnect attempt that sets the wrong value for the internal session state for reconnections.

  [#LC0259]

- Opening a published application and then running the explorer.exe command to open Windows Explorer can cause the desktop to open instead of Windows Explorer.

  Note: After installing this fix, the explorer.exe process might exit unexpectedly. For more information, see Knowledge Center article CTX128009.

  [#LC0285]

- Files can become corrupted when copying files between UNC paths of two mapped drives if the second drive is created by using the Windows Substitute command (SUBST) from the first UNC drive.

  [#LC0288]

- With "Multi-Stream" policy enabled, the clipboard data transfer from the server to the user device might take a long time.

  You can create the following registry key to change the default server output bandwidth to a greater value:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
  Name: InitialOutputSpeed
  Type: REG_DWORD
  Value: 10000 – 1000000 (10KB/s - 1000KB/s; recommended value: 300000)

  [#LC0390]

- After configuring Excelhook as described in Knowledge Center article CTX133198, in sessions where both Microsoft Excel and Microsoft VB for Applications are running, the following issues can occur:

  - The main Excel window remains in the foreground even when the VB for Applications window has focus.
  - Closing the VB for Applications window also closes the main Excel session.

  [#LC0398]

- User sessions might stall in a disconnected state during log off. As a result, the sessions cannot be closed and you cannot

restart the server.

[#LC0399]

- Attempts to publish Mozilla Firefox 28 and later versions in XenApp can fail with the following error message:

  "System.NotSupportedException: Data is not in ICO format"

  [#LC0402]

- Citrix XenApp 7.6 and XenDesktop 7.6 VDA Core Services running on Windows Server 2008 R2 (Server OS) might become unresponsive at the "Welcome" screen. If this occurs, new Receiver and Remote Desktop (RDP) connections to the server fail.

  [#LC0405]

- Occasionally, user sessions might become unresponsive and can fail to log off. This also occurs if users log off manually from the console.

  [#$LC0472]

- In published desktops, the status indicator progress bar might fail to complete and certain logon status messages might fail to appear when users log on or launch applications.

  [#LC0482]

- The "Automatic keyboard display" on mobile devices (such as iOS and Android) appears unexpectedly during screen transition in the Microsoft Silverlight web application.

  [#LC0499]

- When users close a published version of Visual Basic Editor from the taskbar, open published Excel spreadsheets also close.

  [#LC0534]

- When starting a published application, users can experience slow logons.

  [#LC0596]

- If the "Mobile Experience" policy is enabled in XenApp 6.5, when users connect with Receiver for iOS, the following error message appears when users log off:

  "There was a problem logging off. Please contact the help desk for assistance."

  [#LC0628]

- Attempts to connect to XenDesktop 7.x running on Windows Server 2008 or Windows Server 2012 VDAs might fail if the user password contains more than 45 characters.

  [#LC0689]

- Time zone synchronization might not work with published Java applications in sessions running on non-English Windows 7 user devices when the option "Allow time zone redirection" is enabled. The issue occurs because the GetDynamicTimeZoneInformation API cannot return the time zone information to the Receiver session.

  On international language user devices, set the system locale to the same language as the language pack.

Note: This fix does not address the issue for Russian time zones.

[#LC0807]

- With client drive mapping enabled, unexpected characters are occasionally appended to the end of files written by a published VB application using the FileStream() function.

  [#LC0815]

- On the user device, attempts to remote the combo box control under Region and Language > Date and Time formats might fail. This can occur when the combo box control has been successfully remoted once and a second attempt is made to remote it.

  [#LC0836]

- When users attempt to connect to a disconnected session, it can take up to three minutes to establish the connection.

  [#LC0850]

- When launching a published application, the following error message can appear on the user device:

  "The Citrix server is unable to process your request to start this published application at this time. Please try again later. If the problem persists, contact your administrator."

  Background: It can take some time for the wfshell process to finish checking application properties before launching the application. Depending on network conditions, the request can timeout before the check is complete and the error message appears.

  This fix introduces support for the following registry key that allows you to delay the timeout of the application properties check to up to four minutes:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICAST
  Name: WaitTimeOutValue
  TYPE: REG_DWORD
  Value: <desired timeout delay, in milliseconds. Default: 12000; max value supported: 240000>

  [#LC0860]

- When users log on with any version of Receiver for mobile devices and then open a published version of Lotus Notes where the "Automatic Keyboard Display" policy is enabled, when entering email addresses in the "To," "CC," and "BCC" fields, the keyboard does not appear.

  [#LC0899]

- A "Connection Established, Negotiating Capabilities" pop-up window appears from the Receiver when the VDA becomes unresponsive. To start any other sessions successfully, restart the VDA.

  [#LC0909]

- The time zone is not correct when users log on with Receiver for Windows. For this hotfix to work correctly, you must install the following:

  - The same Microsoft time zone update hotfix on the user device and the server. For example, if Microsoft Hotfix KB2998527 is installed on the user device, install this hotfix on the server.

- Microsoft Hotfix KB2870165 on the server if the server operating system is Windows Server 2008 R2 Service Pack 1.
- Fix #LC1392 is installed on the user device.

[#LC1061]

- Attempts to reconnect to an active session on the server might fail. With the application instance limit set to "1," attempts to open another session can fail and the user must either log off or disconnect from the existing session to be able to reconnect or to be able to start a new session.

  [#LC1084]

- Attempts to enumerate applications can fail if the trust relationship between domains changes while servers that belong to the farm are shut down. Attempts to log on using a UPN succeed, but attempts using a down-level logon name fail.

  [#LC1136]

- If the USB redirection policy contains more than 1000 characters all USB drives are redirected, even if there is a deny rule for the device.

  [#LC1153]

- When ExcelHook is enabled and multiple projects are opened in Microsoft Project 2013, the first project opened might not appear in the taskbar.

  [#LC1158]

- Occasionally, the visual settings, such as caption font, scroll bar size, and menu height, of seamless applications might not synchronize correctly with the user device settings.

  [#LC1169]

- Session sharing can fail intermittently.

  [#LC1184]

- If another process holds the same lock as picadm.sys, users cannot log off from the session and the session remains in a disconnected state.

  [#LC1243]

- The final image quality might degrade if the settings "Build to lossless" and "Allow Visually Lossless Compression" are enabled on the Desktop Delivery Controller (DDC).

  [#LC1271]

- When users log on for the first time, the screen might appear corrupted in the Receiver session. The issue occurs when you change Visual quality to "Build to lossless" and enable the "Allow visually lossless compression" setting.

  [#LC1272]

- Attempts to copy information fail in a published version of Microsoft Access 2007. The information does not appear in the Office clipboard.

  [#LC1290]

- The published version of Microsoft Excel 2010 fails when moving between open spreadsheet files.

[#LC1356]

- Redirection might not work correctly for the MailTo feature in XenDesktop and XenApp sessions. When the user clicks on the "MailTo" link in the web browser, instead of opening the published Microsoft Outlook, an error appears.

  [#LC1400]

- When Session Lingering is enabled and an application is closed on an iOS or Android device, a black window appears and stays on the device screen.

  [#LC14074]

- When a user reconnects to a session using auto client reconnect, the client-side time zone might fail to be redirected in the user device and the server-side time zone might appear on the user device instead.

  [#LC1426]

- When users reconnect to their desktop session, the values for "Session Creation Server Duration (SCSD)" and "Session Startup Server Duration (SSSD)" are not reset.

  [#LC1464]

- On a German Windows-based device, the Multimedia Rave (RaveEventMessages.dll) service for the German language can make the svchost.exe process that holds the event log service to fail. When this occurs, users cannot log on.

  [#LC1543]

- When users start a published application, the Citrix Stack Control Service (SCService64.exe) stops responding.

  [#LC1545]

- When users log off from a desktop session, WFShellWindow stops responding and the message "Wfshell needs to close" appears for three minutes.

  [#LC1591]

- In a multi-monitor environment, the application might open behind the published seamless toolbar application.

  To enable the fix, installation of Fix #LC1342 and Fix #LC0491 might be required.

  [#LC1673]

- When logging on to a Windows-based device and then connecting to XenApp virtual machines (VMs), the TWI module (TWI3.dll) increases CPU usage.

  [#LC1810]

- In two dual-monitor user device setups, if several applications with HDX features are started, some of those applications might appear as black windows.

  [#LC1818]

- When recording a XenApp session where Legacy Graphics mode is disabled, recording files cannot be rolled over.

  [#LC1850]

- A time-out can occur in a lingering session and can cause the session to quit unexpectedly resulting in a black window.

  [#LC1903]

- When users attempt to connect to a disconnected session, it can take up to three minutes to establish the connection.

  [#LC1908]

- If Active Directory servers are set as Read-Only servers, users cannot start applications and the message "Connection Established, Negotiating Capabilities" appears indefinitely.

  [#LC1964]

- When the "Auto Client Reconnect" policy is enabled in a session, the authentication prompt might not appear.

  To enable the fix, set the following registry keys:

  - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\WFShell
    Name: SessionReconnectMinTimeInMilliSeconds
    Type: REG_DWORD
    Value: the maximum session length
  - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\WFShell
    Name: LockOnReconnect
    Type: REG_DWORD
    Value: 1

  After configuring the registry key, restart the server or run the command "gpupdate /force."

  [#LC1990]

- When launching published applications, the Citrix Graphics (CtxGfx.exe) process can cause CPU consumption to be higher than normal.

  [#LC2007]

- Session screen resolution might fail to resize when users disconnected from a session using Citrix Receiver for Windows and reconnect to the same session, on a device with a smaller screen resolution, using Citrix Receiver for Linux or Citrix Receiver for Windows CE. This can occur when the "Legacy graphics mode" policy setting is enabled for the session.

  [#LC2079]

- When users copy the contents of an embedded Word file that is opened from within SAP, pasting the content into a new embedded Word file fails.

  [#LC2092]

- When users start a published desktop from the Web Interface, the session becomes unresponsive at "Setting up personalized settings for: Microsoft Windows Media Player" and audio does not work from the desktop.

  [#LC2103]

- If Lotus Notes is started on an iPad with Receiver for iOS, the application might close unexpectedly.

  [#LC2124]

- Attempts to reconnect to a disconnected session occasionally fails because the session attribute "AllowReconnect" is set

to "False."

[#LC2174]

- When users disconnect from a session, Citrix WinFrame Shell (WFShell.exe) causes high CPU utilization.

  [#LC2235]

- Internet Explorer launched as a published application with the the /appve argument fails to load the associated package.

  [#LC2292]

- Wfshell.exe continues to use a large amount of CPU resources after users disconnect from a session.

  [#LC2391]

- When using AutoCAD and AutoCAD Civil 3d, the mouse pointer permanently displays as an hour glass.

  [#LC2438]

- When opening a published application file from a Client Drive Mapping (CDM) and then saving the file after entering text, the modified time stamp does not update.

  [#LC2305]

- Attempts to work on a file that resides on a Client Drive Mapping (CDM) drive might result in a deadlock on picadm.sys and can cause the published desktop to become unresponsive.

  [#LC2312]

- If an Excel .csv file contains a large number of entries, copying the file from the user device to the server can take a long time.

  [#LC2366]

- When maximizing published versions of Excel or Internet Explorer, the top of the name box, formula bar, or menu bar appear as a white bar.

  To enable the fix for Excel and Internet Explorer, create the following registry keys:

  Excel

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\XLMAIN

  Name: ClassName
  Type: REG_SZ
  Value: XLMAIN

  Name: Type
  Type: REG_DWORD
  Value: 0x00020000

  Internet Explorer

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\IEFrame

Name: ClassName
Type: REG_SZ
Value: IEFrame

Name: Type
Type: REG_DWORD
Value: 0x00020000

To apply this fix to multiple servers, create a registry flag. For more information, see "Seamless Per Application Window Registry Flags" in Seamless_Configuration.pdf on the Citrix Support site.

[#LC2504]

- When Excelhook is enabled, switching between open Excel workbooks can lose the focus on the selected workbook. Additionally, users cannot select any of the open Excel workbooks and the focus stays on the last chosen file.

  #LC2589]

- If the setting "Allow only one instance of application for each user" or the "Auto client reconnect" policy are enabled, users receive the error "You already have an instance of this application open and are not allowed to run more than one instance. Please contact your System Administrator." This occurs because session sharing fails between two forests.

  [#LC2592]

- Videos are blank in the application "Unreal Streaming Media Player" when played in a published version of Internet Explorer 8 on a Windows 7 64-bit computer.

  [#LC2650]

- Copying more than 1,000 files by using client drive mapping might cause performance issues.

  [#LC2702]

- Users cannot start applications after updating cipher registry keys. To apply this fix, install the new version of the SSL SDK.

  [#LC2729]

- Sessions might fail to launch and the following error message might appear:

  "A device attached to the system is not functioning."

  This can occur in Kerberos-secured environments with two-way trust domains when the user and the server are in different domains.

  [#LC2762]

- When opening a published version of Internet Explorer on Windows Phone 8.1, if the device is turned horizontally, half of the screen appears as a blank window. Additionally, users cannot maximize the Internet Explorer window. If users turn the device vertically, the screen appears normal.

  [#LC2786]

- When session sharing and session linger are enabled, disconnected sessions might fail to reconnect to the same VDA, but instead reconnect to a different VDA. When this occurs, event ID 1048, event ID 1050, and event ID 7 are logged on the VDA.

[#LC2860]

- If a published application stops working, the Desktop Window Manager might fail to allow the user to close the application.

  [#LC2922]

- When a user connects to a session on a server, the session might fail to progress beyond the welcome screen. This can occur for all sessions on the server until the server is restarted.

  [#LC2936]

- The key and value in registry location HKEY_CURRENT_USER\Control Panel\Desktop\UserPreferencesMask on the VDA might be overwritten by the wfshell.exe process each time a user logs on to the VDA. To prevent this, create the following registry key on the VDA and set the value to 1:

  HKLM\SYSTEM\CurrentControlSet\Control\Citrix
  DWORD value:
  EnableVisualEffect

  [#LC2965]

- Shortcuts for desktops and download recreated in Windows Explore favorites menu under %userprofile%\Links, after they have been deleted, when the user logs in to the VDA again.

  [#LC2998]

- When users log on and log off repeatedly, the Citrix WinFrame Shell (Wfshell.exe) stops responding.

  [#LC3003]

- When users log on with Receiver 4.2, the time that appears in the session does not match the time on the user device.

  [#LC3067]

- Attempts by administrators to launch applications published from the System32 folder can fail.

  [#LC3148]

- When using an external monitor along with a laptop, a white square can be visible in a corner of the external monitor. The issue arises specifically when the external monitor has a screen resolution different from the resolution of the primary monitor, is located to the left of the primary monitor, and its top edge is above the top edge of the primary monitor.

  [#LC3186]

- Attempts to connect to a disconnected session after placing fully loaded servers in an offline state by using the load evaluator might fail.

  [#LC3226]

- When users connect to a published desktop from Receiver 4.2, Citrix WinFrame Shell (wfshell.exe) fails.

  [#LC3227]

- When starting published applications or desktops on XenApp server, single sign-on might not work.

  [#LC3301]

- With USB Redirection disabled, disconnecting from a published application can cause the following, spurious Event 261 to appear in the Event Viewer:

  "The Citrix Device Redirector service could not complete an IO operation with the Redirector Bus."

  [#LC3439]

- When exiting a 64bit ThinAPP packaged application (BMC Control-M), the application can experience an unexpected exception on sfrhook64.dll.

  [#LC3484]

- On occasion, clipboard redirection fails after you reconnect to a disconnected session. The issue occurs if the Clipboard virtual channel closes unexpectedly at the time of reconnecting.

  [#LC3511]

- SSL connections (HTTPS) might not work properly in a VDA.

  [#LC3535]

Site/Farm Administration

- If the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Logon\DisableStatus is enabled (Value=1), the End User Experience Monitoring (EUEM) metrics of Profile Load Server Duration and Login Script Execution Server Duration might be missing.

  [#LA5764]

- Attempts to check Load Evaluator settings can fail and the following error occurs:

  System.Runtime.InteropServices.COMException (0x80004005): Error HRESULT E_FAIL has been returned from a call to a COM component.

  [#LC0359]

- Multiple XenApp servers restart at the same time instead of restarting at different times as defined in the "Reboot schedule randomization interval" policy.

  [#LC1402]

- Non-administrative users are unable to establish an RDP session to a XenApp 7.6 server when an Remote Desktop Gateway is specified.

  [#LC2371]

- Spurious updates might be made to servers' local host cache after the Microsoft DsBind() API function fails. Symptoms of this issue include rapid increases to the size of the local host cache on controllers and changes to the contents of worker groups pointing to Active Directory OUs.

  [#LC2631]

- The "dscheck /full workergroup" command might report errors incorrectly when verifying Workergroups that do not contain 'Farm Servers' objects, displaying the following message:

"Error:: Failed to retrieve Server UIDs for the WorkGroupUID."

This fix modifies the message displayed in this circumstance to the following:

"This workergroup is configured for Farm Server and has no Server UID, verification OK."

[#LC3383]

- The Reboot schedule randomization interval setting might not be honored for servers provisioned with Provisioning Services.

  [#LC3430]

- When an application is published to a Worker Group, running the command dscheck /full apps /servercheck mistakenly returns the Worker Group object as an unknown server, offering the option to delete it.

  [#LC3556]

Smart Cards

- The Citrix Smart Card Service might cause very high CPU usage. To correct this issue, restart the Citrix Smart Card Service.

  [#LA5919]

- After upgrading VDAs, Microsoft Outlook does not prompt for a personal identification number (PIN) when users attempt to log on with a smart card. Instead, the following error message appears:

  "Please insert a smart card."

  [#LC0556]

- After logging on to a server by using a smart card, the server can become unresponsive at the Welcome screen and refuse to accept new sessions. Restarting the Smart Card Service resolves the issue and the server continues to accept new sessions.

  Configuring the following registry keys might not be necessary if fix #LA0983 is already installed and you configured the registry settings during the previous hotfix installation.

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
  Name: TransactionTimeoutEnable
  Type: REG_DWORD
  Value: 1 (enable)

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
  Name: TransactionTimeoutValue
  Type: REG_DWORD
  Value: <any value more than 5 seconds>

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
  Name: SendRecvTimeout
  Type: REG_DWORD
  Value: Minimum time-out value, in seconds; should be 30 seconds or more. Any lesser value defaults to 30 seconds. This value should be at least 10 seconds more than the "TransactionTimeoutValue."

  [#LC0910]

- After authenticating using Citrix Receiver for Linux while a smart card is present in the reader attached to the endpoint, the session can become unresponsive.

  [#LC0982]

- The ActivIdentity (accompkcs.exe) process might exit unexpectedly with an exception on scardhook64.dll. As a result, the websites that require a smart card might not function until the VDA is restarted.

  [#LC1056]

- The Citrix Smart Card Service might become unresponsive and the users might not be able to log on to the server until the service is restarted.

  [#LC1276]

- Removing a smart card from the reader during session logon can prevent the session from properly terminating on the server. As a result, the server can exhibit a state where smart card logons for any future sessions are prevented.

  [#LC3020]

- When connecting to a published desktop with a smart card, the Citrix Smart Card Service might become unresponsive.

  [#LC3421]

System Exceptions

- The operating system experiences an error on picaser.sys and a blue screen appears with bugcheck code 0x0000000A.

  [#LC0222]

- The operating system experiences an error on picadm.sys and a blue screen appears with bugcheck code 0x22.

  [#LC0227]

- On servers with Hotfix Rollup Pack 3 or 4 installed, Remote Desktop Services can exit unexpectedly on XenApp 6.5 servers that act as XML Brokers.

  [#LC0440]

- Servers might experience a fatal exception, displaying a blue screen, on vdtw30.dll.

  [#LC0471]

- The operating system experiences an error on picadm.sys and a blue screen appears with bugcheck code 0x00000022.

  [#LC0483]

- In sessions on systems with Fix #LA5282 (first included in XA650W2K8R2X64R04 - XenApp 6.5 Hotfix Rollup Pack 4) installed, clicking URLs from within a published application can cause the winlogon.exe process to exit unexpectedly. As a result, the published application disconnects.

  [#LC0523]

- The Citrix XML Service can fail unexpectedly.

  [#LC0548]

- Playing a video in a media player in a pass-through session can cause the session to exit unexpectedly.

  [#LC0553]

- Servers might experience a fatal exception on vdtw30.dll with bugcheck code 0x0000007E appearing on a blue screen.

  [#LC0599]

- The operating system experiences an error on picadm.sys and a blue screen appears.

  [#LC0623]

- Servers might experience an error on picadm.sys and a blue screen appears with bugcheck code 0x0000000A.

  [#LC0649]

- The winlogon.exe process might exit unexpectedly on twi3.dll when logging off from a Remote Desktop (RDP) session.

  [#LC0793]

- VDAs can experience an error on picadd.sys and a blue screen appears.

  [#LC0798, #LC1096]

- The VDA experiences an error on ctxdvcs.sys with bugcheck code E3 that appears on a blue screen.

  [#LC0857]

- The operating system experiences an error on picadm.sys and a blue screen appears with the stop code 0x0000003B.

  [#LC0896]

- Windows Explorer might close unexpectedly in one of the following cases:

  - When selecting a large number of files whose names contain more than 260 characters, and then selecting the "Send to > Fax recipient" option.
  - When attempting to open third party applications.
  - When attempting to combine files by using Nitro PDF.

  [#LC0938]

- A page fault in the ICA WSK Transport Driver (tdwsk.sys) causes the VDA to fail with an error on a blue screen.

  [#LC1032]

- When launching a published application or desktop, the Windows Logon User Interface (LogonUI.exe) or the explorer.exe process might exit unexpectedly on icaendpoint.dll if the Citrix Audio Redirection Service fails to start.

  [#LC1167]

- The operating system experiences an error on picadm.sys and a blue screen appears.

  [#LC1239]

- Servers can exit unexpectedly on vdtw30.dll.

  [#LC1328]

- Servers might experience a fatal exception, displaying a blue screen, on vdtw30.dll.

  [#LC1414]

- An error on twi3.dll can cause servers to stop responding.

  [#LC1417]

- The svchost.exe process for Terminal Services might close unexpectedly with an application Event ID 1000 and can cause the Remote Desktop and Receiver connections to the server to fail.

  [#LC1419]

- The operating system experiences an error on picadm.sys and a blue screen appears. The issue occurs when the value of "TrucationResource" becomes null.

  [#LC1430]

- An error on vdtw30.dll can cause bugcheck error 0x0000003B, {c0000005, fffff96000863133, fffff880099aaf70, 0} that appears on a blue screen.

  [#LC1567]

- The server can experience a deadlock on picadm.sys that prevents the server from accepting new user connections.

  [#LC1685]

- The Citrix Stack Control service exits unexpectedly if there is an invalid session key.

  [#LC1717]

- Playing an audio file from Receiver for HTML5 where SSL is enabled in the ICA session can cause the VDA to experience a fatal exception. displaying a blue screen.

  [#LC1752]

- The svchost.exe process might stop unexpectedly due to the ICA Audio Endpoint dll (icaendpoint.dll).

  [#LC1775]

- Occasionally, the VDA might unexpectedly shut down and then restart.

  {#LC1876}

- Terminal Services might close unexpectedly due to RPM.dll.

  [#LC2031]

- Servers might experience a fatal exception on vdtw30.dll with bugcheck code 0x0000003B appearing on a blue screen.

  [#LC2037]

- The operating system experiences an error on ctxdvc.sys and a blue screen appears with bugcheck code 3B.

  [#LC2119]

- The operating system experiences an error on tdica.sys and a blue screen appears with bugcheck code 44

[MULTIPLE_IRP_COMPLETE_REQUESTS].

[#LC2171]

- Windows Server 2008 R2 and Windows Server 2012 R2 might experience a fatal exception when users connect with Receiver for Windows.

  [#LC2179]

- An error on picadm.sys with bugcheck code 0x00000022 appears on a blue screen.

  [#LC2236]

- The winlogon.exe process might close unexpectedly on twi3.dll.

  [#LC2244]

- The operating system experiences an error on picadm.sys and bugcheck code 0x00000022 appears on a blue screen.

  [#LC2265]

- The VDA servers experience an error on icardd.dll and a blue screen appears.

  [#LC2277]

- On servers with Hotfix Rollup Pack 5 installed, Remote Desktop Services can exit unexpectedly on XenApp 6.5 servers that act as XML Brokers.

  [#LC2376]

- Servers might experience a fatal exception on ctxdvcs.sys with bugcheck code 0x0000003B appearing on a blue screen.

  [#LC2444]

- A Windows Explorer process might terminate unexpectedly during a published desktop session and the error message "Windows Explorer has stopped working" might appear.

  [#LC2733]

- When a point-of-sales device is redirected to a shared desktop through the COM port, the device might not be recognized by third-party software running on the shared desktop.

  [#LC2775]

- Servers might experience an error on icausbb.sys and with the message PNP_DETECTED_FATAL_ERROR appearing on a blue screen.

  [#LC2811]

- The wfshell.exe process might close unexpectedly and prevent new connections.

  [#LC3024]

- Servers might experience a fatal exception on vdtw30.dll and win32k.sys with an error appearing on a blue screen.

  [#LC3103]

- After enabling the "client clipboard redirection" policy, the wfshell.exe process might close unexpectedly.

  [#LC3249]

- VDAs might experience a fatal exception on vdtw30.dll, displaying a blue screen.

  [#LC3354]

- The csrss.exe process can experience a fatal exception on vdtw30.dll with stop code 0x7e.

  [#LC3482]

User Experience

- This fix addresses a usability issue with Desktop Composition Redirection with Receiver for Windows prior to Version 4.200 when used over LAN connections.

  [#LC1507]

- This release includes an enhancement that allows users that log on with Receiver for HTML5 or Receiver for Chrome to transfer files through remote sessions and local devices.

  [#LC3014]

User Interface

- This fix addresses the following issues with the way applications are represented in the Receiver for Windows taskbar:
  - Individual applications can display the default Receiver icon instead of the application-specific icon.
  - When multiple applications are running in the same session, they can appear grouped under a single, default Receiver icon.

  [#LC0094, #LC1181]

- With the "Remote the combo box" policy enabled, when users open Internet Explorer in Receiver for iOS using an iPad, the balloon for the remote combo boxes does not appear correctly. For example, when clicking combo box B, the balloon appears to come from combo box A.

  [#LC1800]

- Certain borders of the seamless application window might be hidden. The issue occurs when the "GetWindowRect" function fails to get the correct size of the window and as a result, the window coordinates appear without border.

  [#LC1943]

- The "Automatic Keyboard display" might not appear when users open a published application from Receiver for Windows or mobile Receivers.

  [#LC2747]

Miscellaneous

- This fix provides general compatibility improvements with Microsoft updates.

  [#LA5638]

- This fix addresses a memory issue in an underlying component.

[#LA5765]

- When attempting to retrieve the license server address, incorrect characters appear in the license server name.

  [#LC0363]

- This fix addresses handle leaks in the WMI process.

  [#LC0662]

- This fix addresses a stability issue with Special folder redirection and file names that contain more than 205 characters.

  [#LC0719]

- This fix addresses a memory issue in an underlying component.

  [#LC0732, #LC0800, #LC0953, #LC2764, #LC2888]

- When users start a published version of Excel and then sends the file by using "Send Using E-mail," when users type text and then press the Backspace key a few times in Outlook, Chinese characters are inserted instead of a backspace.

  [#LC1155]

- COM port signature pads with USB adapters do not work correctly when users log on with Receiver for Mac. The signature pads do work correctly when users log on with Receiver for Windows.

  [#LC1396]

- A handle leak in CTXCDF causes the Windows Management Instrumentation Provider Service (WMIPRVSE.exe) to stop. and EventID 5612 appears in the event log.

  [#LC1764]

- This fix addresses memory leaks in the Citrix Audio Redirection Service (CtxAudioSvc).

  [#LC2054]

- The Powershell command "Get-BrokerSession | Format-List -Property SessionState" shows incorrect session status. For example, disconnected connections show as an active session.

  [#LC2080]

- This release includes support for the Framehawk Virtual Channel, a new ICA virtual channel that extends Citrix HDX technologies to improve user experience on broadband wireless connections where packet loss and latency are common issues. For more information, see What's new.

  [#LC2782]

- This enhancement improves the message for Event ID 1480 and includes the following information:

  - Published app name
  - Command line
  - User ID

- User domain
- Client name
- Session ID

[#LC2830]

- Creation of the sessionchange.log file on the root of C: drive of the VDA cannot be disabled or moved to a different location.

  [#LC3621]

Known issues

Sep 23, 2016

Feature Pack 3

- In recent Firefox versions, the browser add-ons for URL redirection are disabled by default, so you must enable them. This is a third-party issue. [#283844]
- Users cannot open some files from redirected folders such as Downloads and Desktop, if they downloaded the files using the Edge browser within a Windows 10 VDA. To work around this issue, use Internet Explorer to download files. [#591635]
- The following registry keys are not present after upgrading a brokerless VDA to FP3, and must be added manually [#591030]:
  - hklm\software\citrix\VirtualDesktopAgent\HaModeComputerName
  - hklm\software\citrix\VirtualDesktopAgent\HaModeTimeEnd
- When using Receiver for Windows with a Wacom pen device on a Windows 10 VDA, if you lose the network connection, the cursor may fail to display once the session is reconnected (using Automatic Client Reconnection, ACR). To work around this issue, disconnect and reconnect the session. [#593516]
- Persistent CDF tracing is not available if the Citrix Telemetry Service is running. To work around this issue, temporarily disable the Citrix Telemetry Service. [#593347]
- There is an error in XenApp and XenDesktop 7.6 FP3, when you update an existing Windows 10 master image on XenServer to use the XenServer hotfix XS65ESP1010 with XenTools. [#593985]
- Apps which are published from a Windows 10 VDA do not display their full borders when maximized [#593596]. To work around this issue, registry keys can be set for each application class. For example, to work around the behavior for Paint, you create the following key:

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\MSPaintApp]

  "ClassName"="MSPaintApp"

  "Type"=dword:00020000

  Note that you must add the Class Name for an application, not the application name. For example, for Paint add **MSPaintApp**. You can get the Class Name using a tool such as Spy++. For more information on Seamless Configuration Settings, see CTX101644.

- Some "Learn more" help links may not redirect correctly to the current Product Documentation site (docs.citrix.com). To work around this issue, access the Product Documentation site directly. All documentation for 7.6 FP3 and earlier 7.6 feature packs is on the new Product Documentation site under XenApp and XenDesktop 7.6.
- Temp files from the standalone VDA installation package remain in the VDA Operating System's temp folder after completion of the install. To work around this issue, manually delete the temporary files. [#594829]

Feature Pack 2

Linux Virtual Desktop

Rich-text formatting is lost when text is copied from an application within the session and pasted into an application outside of the session, and when it is copied from outside the session and pasted inside. [#0538497]

Host names (the host part of the fully qualified domain name, or FQDN) longer than 15 characters are truncated, preventing successful VDA registration. [#0544120]

Linux VDA registration status fails to change on the endpoint when resuming from hibernation. During a power cycle event, the endpoint fails to obtain an IP address, which prevents it from registering. [#0569303]

The Linux VDA does not currently support DNS lookup of realm mappings. [#0557555]

KDE-based applications appear unavailable in Linux VDA sessions. [#0568006]

Linux VDAs running RedHat Enterprise fail to connect if Quest authentication service is enabled and SELinux is in enforcement mode. [#0551761]

Framehawk Virtual Channel

Citrix Receiver for Windows (Version 4.3) and Citrix Receiver for iOS Classic (Version 6.0) are the only Receiver platforms currently supported.

Session Recording/Smart Auditor are not supported with Framehawk.

This release of Framehawk is designed for standard XenApp and XenDesktop workloads, such as knowledge worker and office apps. It has not been tested with high-end graphic intensive environments

Multi-monitor clients are not supported at this time.

The Vd3dn.dll may crash on the client under test conditions, such as modifying bandwidth and latency on a WAN emulator in-session. Disconnect the session before making any changes to WAN emulator settings, then reconnect; Framehawk recalibrates during session handshake.

If the Framehawk policy and the legacy policy are both enabled, the Framehawk policy takes precedence on Workstation operating systems (for example, Windows 7); for RDS environments (for example, Windows 2012 R2), the legacy policy is applied.

For Windows 7 environments, the initial XenDesktop 7.6 FP2 release of Framehawk does not provide touch support (for example, pinch and zoom), despite this functionality being present in a Windows 7 OS. Additionally, Windows 2008 R2 does not provide touch support.

StoreFront 3.0

For the StoreFront 3.0 known issues and fixed issues, see the StoreFront 3.0 documentation known issues and fixed issue.

HDX RealTime Optimization Pack 1.8

For the HDX RealTime Optimization Pack 1.8 known issues and fixed issues, see the Optimization Pack 1.8 documentation known and fixed issues.

Feature Pack 1

Session Recording

- When Machine Creation Services (MCS) or Provisioning Services creates a VDA with configured master image and Microsoft Message Queuing (MSMQ) installed, the VDA has the same QMId as the MSMQ. This might cause various issues, such as:
  - Sessions mighty not be recorded even if the recording agreement is accepted.
  - The session logoff signal might not be received by the Session Recording server, which leads to the session always in Live status. [#528678]

  The workaround to create a unique and persistent QMId for each VDA is to use a script. To use the script, do the following:

1. Make sure the execution policy is set to RemoteSigned or Unrestricted, in PowerShell.
   Set-ExecutionPolicy RemoteSigned
2. Create a scheduled task and set the trigger as At system startup and run with SYSTEM account on the Provisioning Services or MCS master image machine.
3. Add the command as a startup task.
   powershell.exe -file C:\GenQMID.ps1

> ### Warning
>
> Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Summary of the script:

1. Generate the QMid based on the hash value of the machine FQDN.
2. Stop related services, including CitrixSmAudAgent and MSMQ.
3. Set the QMid in the registry.
4. Start services that stopped previously to apply QMId's change.

This script is for reference COPY

```
<p>function ConvertHexStringToByte($theString)&amp;nbsp;<br>
{&amp;nbsp;<br>
$bytes = New-Object Byte[] ($theString.Length / 2)&amp;nbsp;<br>
for ($i = 0; $i -lt $theString.Length; $i += 2) {&amp;nbsp;<br>
$bytes[$i / 2] = [System.Convert]::ToByte($theString.Substring($i, 2), 16)&amp;nbsp;<br>
}&amp;nbsp;<br>
return $bytes&amp;nbsp;<br>
}&amp;nbsp;<br>
<br>
Try {&amp;nbsp;<br>
# Get UUID of machine&amp;nbsp;<br>
$strUUID = (Get-WmiObject -Class Win32_ComputerSystemProduct | Select-Object -Property UUID).UUID&amp;nbsp;<br>
<br>
# Remove &amp;quot;-&amp;quot;&amp;nbsp;<br>
$strUUID = $strUUID.ToString().Replace(&amp;quot;-&amp;quot;, &amp;quot;&amp;quot;)&amp;nbsp;<br>
<br>
# Convert string to bytes&amp;nbsp;<br>
$UUID = ConvertHexStringToByte($strUUID)&amp;nbsp;<br>
<br>
# Set UUID as QMId&amp;nbsp;<br>
$new_QMID = $UUID&amp;nbsp;<br>
} Catch {&amp;nbsp;<br>
# If exception occurred, just use MD5 digest of FQDN as QMID&amp;nbsp;<br>
<br>
# Get FQDN&amp;nbsp;<br>
$fqdn = [System.Net.Dns]::GetHostByName(($env:computerName)).HostName&amp;nbsp;<br>
<br>
# Calculate MD5 hash of FQDN&amp;nbsp;<br>
$md5 = new-object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider&amp;nbsp;<br>
<br>
# Set md5 digest as QMID&amp;nbsp;<br>
$utf8 = new-object -TypeName System.Text.UTF8Encoding&amp;nbsp;<br>
$new_QMID = $md5.ComputeHash($utf8.GetBytes($fqdn))&amp;nbsp;<br>
}&amp;nbsp;<br>
<br>
# Write new_QMID into registry&amp;nbsp;<br>
Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name &amp;quot;QMId&amp;quot; -Value $new_QMID&amp;nbsp;<br>
<br>
# Restart MSMQ to adopt new QMId&amp;nbsp;<br>
<br>
# Get dependent services&amp;nbsp;<br>
$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name&amp;nbsp;<br>
<br>
Restart-Service -force MSMQ&amp;nbsp;<br>
<br>
# Start dependent services&amp;nbsp;<br>
if ($depServices -ne $null) {&amp;nbsp;<br>
foreach ($depService in $depServices) {&amp;nbsp;<br>
$startMode = Get-WmiObject win32_service -filter &amp;quot;NAME = '$($depService.Name)'&amp;quot; | Select -Property StartMode&amp;nbsp;<br>
if ($startMode.StartMode -eq &amp;quot;Auto&amp;quot;) {&amp;nbsp;<br>
Start-Service $depService.Name&amp;nbsp;<br>
}&amp;nbsp;<br>
}&amp;nbsp;<br>
}</p>
```

- When recording a session with a resolution higher than or equal to 4096 x 4096, there might be fragments in the recording appearance. [#524973]
- When you change your XenApp or XenDesktop license type, the change does not take effect immediately for Session Recording. Workaround: Restart the VDA machine. [#532393]
- You might receive an Installation failed error in the following two cases. You can ignore the message, but to avoid receiving the message, restart the machine before reinstalling the Session Recording components. [#544579]
  - Uninstalled the Session Recording components, and then reinstalled them without restarting the machine.
  - Installation failed and rollback happened, and then you tried to reinstall the Session Recording components without restarting the machine.
- Limitation for Session Recording to support the Pre-Launched application sessions [BUG0561109]
  - Problem:
    - If the active policy tries to match the application name, the application launched in the pre-launched session will not be matched, which results in the session not being recorded.
    - If the active policy records every application, when the user logs into the Windows Receiver (at the same time the pre-launched session is established) a notification for recording will appear and the empty session and any applications that will be launched in this session later will be recorded.
  - Workaround:
    - Publish the applications in separate Delivery Groups according to their recording policy. Do not use the application name as the recording condition. This will ensure pre-launch sessions will be recorded. However, notifications will still appear.

- When recording a session with a resolution higher than or equal to 4096 x 4096, there might be fragments in the recording appearance. [#524973]
- When you change your XenApp or XenDesktop license type, the change does not take effect immediately for Session Recording. Workaround: Restart the VDA machine. [#532393]
- You might receive an Installation failed error in the following two cases. You can ignore the message, but to avoid receiving the message, restart the machine before reinstalling the Session Recordi
  - Uninstalled the Session Recording components, and then reinstalled them without restarting the machine.
  - Installation failed and rollback happened, and then you tried to reinstall the Session Recording components without restarting the machine.

- When recording a session with a resolution higher than or equal to 4096 x 4096, there might be fragments in the recording appearance. [#524973]
- When you change your XenApp or XenDesktop license type, the change does not take effect immediately for Session Recording. Workaround: Restart the VDA machine. [#532393]
- You might receive an Installation failed error in the following two cases. You can ignore the message, but to avoid receiving the message, restart the machine before reinstalling the Session Recordi
  - Uninstalled the Session Recording components, and then reinstalled them without restarting the machine.
  - Installation failed and rollback happened, and then you tried to reinstall the Session Recording components without restarting the machine.

- When recording a session with a resolution higher than or equal to 4096 x 4096, there might be fragments in the recording appearance. [#524973]
- When you change your XenApp or XenDesktop license type, the change does not take effect immediately for Session Recording. Workaround: Restart the VDA machine. [#532393]
- You might receive an Installation failed error in the following two cases. You can ignore the message, but to avoid receiving the message, restart the machine before reinstalling the Session Recordi
  - Uninstalled the Session Recording components, and then reinstalled them without restarting the machine.
  - Installation failed and rollback happened, and then you tried to reinstall the Session Recording components without restarting the machine.

Citrix Licensing 11.12.1

For the Citrix Licensing 11.12.1 known issues and fixed issues, see the Citrix Licensing 11.12.1 documentation known and fixed issues.

HDX RealTime Optimization Pack 1.7

For the HDX RealTime Optimization Pack 1.7 known issues and fixed issues, see the Optimization Pack 1.7 documentation known and fixed issues.

XenApp 7.6 and XenDesktop 7.6

General issues

The following note applies to any workaround that suggests changing a registry entry:

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

- On Server OS machines, the CreateAnonymousUsersApp tool may not delete all anonymous user accounts from the local machine; all anonymous users are local users, not Active Directory users. Because the tool deletes passwords and profiles, any anonymous-user account names that are not deleted are no longer useable. To delete unwanted anonymous-user account names locally on the server, use Manage User Accounts or Computer Manager. [#4999679]
- To configure a nonstandard HTTP/SOAP port for the Universal Print Server web service, use PowerShell cmdlets to change the session printer policy. For information about configuring Group Policy settings, see the Group Policy SDK usage section in the
  — About the SDK
  document. To set the policy value, use:
  Set-ItemProperty LocalGpo:\Computer\Unfiltered\Settings\ICA\Printing\UniversalPrintServer\UpsHttpPort -name Value -Value <portnumber>. [#268593]
- After a Hyper-V host is unpaused, Microsoft System Center Virtual Machine Manager (VMM) might not update the overall host state immediately. This can affect the use of Machine Creation Services (MCS). If one Hyper-V host reports a paused state, that host will not be used to provision Virtual Machines (VMs); if all hosts report a paused state, catalog creation will fail.
  As a workaround, manually refresh the parent cluster node or Hyper-V host node. Also, running environment tests on the host will identify hosts reporting a paused state. [#285696]
- Brokering hosted applications on Desktop OS machines is not supported using the Remote Desktop Protocol (RDP). [#377108]
- This release does not support mounting an .iso file when Client Drive Mapping (CDM) is configured for Windows 8 sessions. [#333111]
- If the Citrix Universal Print Server fails because of bad drivers, try running those drivers under printer driver isolation. For information about how to configure printer driver isolation, see MSDN: http://msdn.microsoft.com/en-us/library/windows/hardware/ff560836(v=vs.85).aspx. [#381460]
- The Enhanced Desktop Experience policy setting does not affect pre-existing user or administrator profiles. As a workaround, delete all pre-existing profiles before enabling/disabling the setting, and delete the profile used for VDA installation (after installing the VDA). If the built-in administrator's account was used for (Virtual Delivery Agent (VDA) installation, you cannot delete the profile. In that case, the user can choose the Citrix Enhanced Desktop Theme when logged on. {#363736]
- If monitor resolution is affected because the VDA desktop session resolution exceeds the client monitor resolution, change the resolution setting on the VDA desktop to the highest supported value for the attached monitor. Alternatively, you can detach the monitor cables from the VDA graphics card. [#365877]
- Screen savers and the power-save option are disabled in sessions. Edit the registry and create the following DWORD value:
  HKLM\Software\Citrix\Graphics\SetDisplayRequiredMode = 0
  This change does not prevent the remote machine screen saver or power save mode from coming on. If the power save mode comes on, the remote session is not updated until the user provides input (mouse/keyboard), but the screen will not be blanked. [#380550]
- Attempting to use a PowerShell SDK New-ProvScheme command or any MCS command from a remote machine before setting the host admin address might result in an error. Set the admin address using the Set-HypAdminConnection command before running the New-ProvScheme command. [#336902]
- This release does not support using this product with Microsoft RemoteFX vGPU feature in a Hyper-V host. Instead, use RDP to access RemoteFX functionality such as Hyper-V vGPU. [#375577]
- Director reports the number of GPU machines that have failed to start in the Machine Failure panel on the Dashboard page. However, this information is not displayed when you drill down to view details on the Filters page.

  You can also view this information in the Historical trends graph. [#0434722]
- If more GPU machines are provisioned or assigned than the XenServer resource pool can support of the GPU type specified, GPU machines may fail to start. Users assigned to a machine (including those using Personal vDisk) that failed to start may not be able to access their virtual desktop through StoreFront. [#0434505]
- If you power on a GPU machine and it fails to start, you may see the following error message:

  Exception Failure in PowerOn, PGPU_INSUFFIENT_CAPACITY_FOR_VGPU

  This indicates that there are insufficient GPU Resources to start another machine that uses the GPU. [#434509]
- If multiple users log on to a Desktop OS machine using RDP and ICA protocols and a user locks his/her RDP session, users connecting through ICA cannot log on to the session. To prevent this issue, users should disconnect or log off RDP sessions when they are finished. [#392311]
- When you publish an application with a Windows 8 VDA host and the application shows non-ASCII characters in the notification area, other unrelated characters might also appear in the notification area after reconnection. To resolve this issue, log off from the session and then launch the application again. [#387963]
- The ability to disable session sharing through a registry entry is not supported in this release. As a result, session sharing is always enabled. If the registry key is set to disable session sharing, the first application launches, but subsequent applications do not launch. There is no workaround for this issue. [#383718]
- When a user reconnects to a disconnected session on Windows Server 2012, there is a memory leak in the Desktop Window Manager. If users connect and disconnect frequently to long-lived sessions, such as in the case of an employee using the same session from work and home, this can cause memory resources on the server to be reduced, eventually leading to slow response times and possibly even server failure. This is a third-party issue in the Microsoft code. For information, see: http://support.microsoft.com/kb/2855336 (to be published in July 2013). [#374261]
- The Help About topics fail when working through Windows PowerShell 3.0. This is a third-party issue with Microsoft. Other help topics are unaffected. [#408866]
- When upgrading from XenDesktop 5 to this release (or to XenDesktop 7.1 or XenDesktop 7.0), a hosted application assigned to both Shared and Private Delivery groups produces a Delivery Group incompatibility error during upgrade. To avoid this error, do not assign hosted applications to both Shared and Private Delivery Groups. [#419424]
- If the Profile management feature is enabled, logon scripts for sessions running Windows Server 2012 R2 or Windows 8.1 are delayed by five minutes by default. Once the session is available, the Logon duration for logon scripts step is not available in Director. The delay is controlled by the Configure Logon Script Delay policy (Enabled = 0). [#407978]
- Desktops may not launch on computers running Windows 8.1 with Microsoft Software Update Management installed. To avoid this, in the Windows 8.1 **Taskbar and Navigation properties**

dialog box, on the **Navigation** tab, select all the options in the **Start screen** section. [#408439]

- If you receive the error "You cannot access this session because no licenses are available" when you try to connect through Remote Desktop Protocol to a brokered session, disable these settings in C:\inetpub\wwwroot\Citrix\Store\App_Data\default.ica: [#422212 and #403855]
  - RDPConnection=false
  - RDP-RedirectDrives=false
  - RDP-RedirectDynamicDrives=false
- The value for the Persistent Cache Threshold policy setting is labelled incorrectly, as Kbps, in Studio. The correct value is bits per second (bps). [# 429478]
- When selecting a custom date range for a Configuration Logging report, the calendar displays might be incorrect. [#452399]
- Machines provisioned on Amazon Web Services or CloudPlatform will not be suspended if their Delivery Group Power Management setting is set to Suspend when disconnected. [#453780]
- Connection times (maximum connection timer, connection timer, and disconnect timer) might fail to work on Windows Server 2012 machines containing Windows Server OS VDAs, causing unexpected session time-out behavior. [#471698]
- When the Auto-create generic universal printer policy setting is enabled, the Citrix Print Manager Service (CpSvc.exe) does not create the Citrix Universal Printer generic printer. Hotfixes that address the issue are available as Knowledge Center articles CTX141565 and CTX141566.
- User connections to VDAs running Windows Server 2012 R2 might fail if the **Maximum allowed color depth** Citrix policy setting is enabled. The **Maximum allowed color depth** does not apply to VDA that use a Windows Display Driver Model (WDDM) driver as the primary display driver, such as VDAs running Windows Server 2012 R2.

Installation issues

- `Error 1904. Module C:\Program Files (x86)\Citrix\System32\rpm.dll failed to register. HRESULT -2147010895. Contact your support personnel` occurs when installing or upgrading the Virtual Delivery Agent (VDA) using the Citrix MetaInstaller, the installation of the third-party Microsoft Visual C++ 2005 Runtime component fails, rolls back, and then falsely notifies the MetaInstaller that the installation completed successfully. Because of this, the MetaInstaller continues to install any remaining VDA components until it reaches the post-install component initialization stage. You cannot continue without the Microsoft Visual C++ 2005 Runtime component being present at this stage. To work around this issue, rerun the MetaInstaller VDA installation, which then successfully reruns the Microsoft Visual C++ 2005 Runtime component installation. Alternatively, see http://support.microsoft.com/?kbid=947821 and follow Microsoft's documented solution. [#489633]
- Installing a Virtual Delivery Agent for Server OS might fail with error 1935 because of backward compatibility errors in the Microsoft Visual C++ 2005 Redistributable. See the Microsoft website or run Windows Update to check for fixes. [354833]
- After a successful VDA for Windows Server OS installation, but before the machine restarts, the Windows event log might contain several error messages (such as TermService 1035 or 1036, indicating the Terminal Server listener stack was down or the session creation failed). If there are no other installation failure indicators, you can safely ignore those event log messages. [#374134]
- When upgrading from XenDesktop 5.x, make sure that the XenDesktop 5.x Desktop Studio is closed before running the upgrade. Otherwise, Studio may close unexpectedly during the upgrade. [#389374]
- When upgrading, an administrator who was disabled in XenDesktop 5.6 might move to the later version without a role or scope. Check the Administrators display in Studio and edit administrators, as needed. [#394765]
- If you enable the Profile management feature and users find that their default Windows 8 applications (such as Weather, News, and Bing) start the first time they log on, but not after subsequent logons, you might have to reconfigure this feature. This issue has been observed in environments where the user profile is not persisted and if the folder AppData\Local has not been excluded (the default). As a workaround, add the folders AppData\Local\Packages and AppData\Local\Microsoft\Application Shortcuts as exclusions. [#394802]
- During VDA installation or upgrade on Windows 7, you might see a Windows dialog box prompting you to Restart the computer to apply changes. Click Restart Later to continue the upgrade; do not select Restart Now. [#396553]
- Installing VDAs through Active Directory Group Policy using individual MSIs is not recommended and might fail. Citrix recommends using the startup scripts provided on the product installation media, as described in Install or remove Virtual Delivery Agents using scripts. [#383432, #372136]
- The optimization phase of the Virtual Delivery Agent (VDA) installation might take a long time to complete. In some tests, it has taken about half an hour and may take longer. These instances occur when installing the VDA on an image running a Windows operating system, if, on the installation wizard Features page, Optimize Performance has been selected. This causes the Microsoft Native Image Generator (Ngen) to run. If this occurs, allow the installation process to finish. Citrix recommends that you run Ngen on your VDA base image prior to provisioning virtual desktops to avoid delays caused when it runs in the background of provisioned virtual desktops. [#381437]
- During upgrade, if an error message mentioning PICAIsPorticaV2 entry point not found appears during an upgrade, it can be safely ignored. Complete the upgrade process and restart the machine when prompted. [#423947]
- The VDA for Windows Desktop OS might not install on evaluation versions of Windows 8. The Installation Options screen displays the message "Cannot be installed on this operating system." The issue occurs because the installation program is incorrectly identifying Windows 8 evaluation versions as unsupported operating systems. A hotfix that addresses the issue is available as Knowledge Center article CTX139660. The hotfix lets you patch the installer before running it on Windows evaluation versions.
- During product installation, machines created by Provisioning Services might fail if .NET Framework 3.5 is not present prior to the installation. To work around this problem, make sure that all NET Framework versions 2.0, 3.0, 3.5, 4.0, 4.5, and 4.5.1 are installed. [#442639, #447851]

Server and Delivery Controller issues

- XenDesktop 7.6 includes a new version of the volume worker package for CloudPlatform. Citrix highly recommends updating the volume worker template in your deployment with this new version. When updating, please note that in-place upgrades for this package are not supported. Therefore, you must first fully uninstall the previous package or build a new volume worker template from scratch. [493211]

Remote PC Access issues

- After upgrading from XenDesktop 5.6 FP1, the Remote PC Access Service administrator name may not display correctly. This does not affect operations. [#437948]
- When an office machine has been instructed to hibernate, a subsequent Remote PC Access session launch may fail. As a workaround for desktop machines that display an error message, try launching the session again. For laptops that display a persistent grey reconnecting screen, restart the PC (remotely from the administrator console using Force Shutdown/Force Restart, or locally with the power button); this can result in data loss. [#441154]
- When relying on the Wake-up Proxy rather than Intel Active Management Technology (AMT) or Wake on LAN packets, a machine might fail to wake up. This is a Microsoft System Center Configuration Manager issue. [#441412]
- Starting a VDA from a user device with a smart card reader might fail if the user previously started the VDA from that device and selected Disconnect from the Desktop Viewer. In this case, the user might see the smart card credential screen or the message 'Reading smart card.' As a workaround, choose one of the following:
  - Remove and reinsert the smart card in the reader
  - Click Cancel. Then, in the VDA, press Ctrl+Alt+Del. [#322301]

Studio issues

- Attempting to launch both StoreFront and Studio causes the Citrix console to exit unexpectedly after XenApp and XenDesktop software is installed on a single Windows 2008 R2 SP1 machine. This occurs when launching both StoreFront and Studio; at the end of the installation, from shortcut menus, or if you open StoreFront in the console first, and then open Studio. To work around this issue, force the Native Image Generator (Ngen) to update the .Net native images. To do this, open a command prompt, and then navigate to c:\windows\microsoft.net\framework64\<v2.0.50727>\. Run ngen update /force. This may take several minutes.

Note: The framework64 version number may vary slightly, but it should always start with 2.0.
[#490819]

- Director does not correctly report licensing errors, and Studio is unable to communicate with the license server. This issue may occur if the license server address for a Delivery Site changes while multiple instances of Studio are open and managing the same XenDesktop or XenApp site. To workaround this issue, refresh licensing data in the site by closing all open instances of Studio, reopening a single instance of Studio, and then navigating to the Licensing node. [#492971]
- When using Machine Creation Services (MCS) to provision machines on VMware vSphere, the combination of CPU sockets and cores on the provisioned machines reflects the combination of CPU sockets and cores on the base image used to create the machine catalogs. During MCS catalog creation, if the number of Virtual CPUs selected is higher than the maximum possible on the host, then provisioned machines are created with the maximum possible sockets and cores for that host, without indication to the user. [#331269]
- When using System Center Virtual Machine Manager in a pure IPv6 environment, and using Machine Creation Services to create machine catalogs, all VMs have both IPv4 and IPv6, even if the master VM is configured without IPv4 in the TCP/IP stack. This is a third party issue with Microsoft, and there is no workaround. [#371712]
- When using VMware vSphere in an IPv4 and IPv6 environment with VMware ESX hypervisors configured with VMXNET3network adapters, all VMs have both IPv4 and IPv6, even if the master VM is configured without IPv4 in the TCP/IP stack. This is a third-party issue with VMware, and there is no workaround. [#371712]
- Long machine catalog names and long storage path names might cause a disk attach error in the VMM job window. Microsoft has identified a maximum limit of 255 characters on the length of the file path for VM resources. This issue has been seen when using local storage on a standalone Hyper-V host, due to the long file path used to store the VMs; however, it is not limited standalone Hyper-V hosts. [#359673]
  As a workaround:
  - Create VMM MCS catalogs with short names, especially when the storage is accessed using a long path.
  - Shorten the path to the storage used to store the VMs.
- To change a database to one that was previously used, you must use the SDK; it cannot be done from Studio. [#355993]
  To switch to the Configuration Logging database:
  - Set-LogDbConnection -DataStore 'Logging' -DBConnection $null
  - Set-LogDbConnection -DataStore 'Logging' -DBConnection '<new database connection string>'

  To switch to the monitoring secondary database:
  - Set-MonitorDbConnection -DataStore 'Monitor' -DBConnection $null
  - Set-MonitorDbConnection -DataStore 'Monitor' -DBConnection '<new database connection string>'

  For example, the new database connection string could be:

  'Server=dbserver;Initial Catalog = dbname; Integrated Security = True'

- When you use MCS to provision machines on your hypervisor platform, CPUs are added but no cores. If you change the CPU value during catalog creation, the products licensed on a per CPU basis might need more licenses. For example, your master image has one CPU and four cores and you change the CPU value during catalog creation.
  If, during MCS catalog creation, you select more CPUs than the maximum possible on the host, provisioned machines have the maximum number supported for that host and you are not notified of the difference. For example, a Desktop OS machine can use only two physical CPUs; thus, you will see only two even if more are assigned.

  As a workaround, ensure your master image VM has the same virtual CPU configuration that you want to deploy for the catalog. [#331274]

- When Lync 2013 client is delivered from a Desktop OS machine or Server OS machine, the video chat feature does not work. See XenDesktop 7.x, XenApp 6.x and Citrix Receiver 4.x Support for Microsoft Lync 2013 VDI Plug-in, (http://support.citrix.com/article/CTX138408) for information about using Lync 2013. [#371818]
- When launching a seamless application on a Windows server, the window might not have the Aero theme, even when Enhanced Desktop Experience is enabled.
  - Users launching only seamless applications never get the Aero theme.
  - Users with a mix of seamless applications and desktops get the Aero theme after establishing the first desktop session; then, seamless applications have the Aero theme.

  As a workaround, set the Citrix Enhanced Desktop theme in the default user profile; all users on that VDA get the Enhanced Desktop Experience for their seamless applications. The theme is part of the VDA install and must be set for all VDAs. [#348812]

- Studio messages sent to a Windows 8 machine will display on the Windows 8 Desktop, and not the Windows default (formerly called Metro) display mode. The user must switch to Desktop mode to see the message. This is a third party issue and there is no workaround. [#387356]
- If a Site contains more than one hosting infrastructure object with the same name, the Studio display might not be correct. When you create hosting infrastructure objects (for example, networks and storage), it is best practice to specify a unique name for each. [#384959]
- After using Delegated Administration to create an administrator with a new scope, refresh the Studio display. Otherwise, you might receive a permissions error when you log on as the new administrator and attempt to create a new connection or resource. [#386634]
- Applications hosted on Desktop OS machines with random assignments might fail to open after the loading dialog box disappears. This issue occurs when the time the application takes to start exceeds the default one-minute time-out and the session exits automatically. [#389025]
  As Administrator, change the base image and re-provision with a changed timeout value as follows:

  Locate the registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI (Create the key if it is not available.)

  Name: ApplicationLaunchWaitTimeoutMS

  Type: REG_DWORD

  Data: Required additional time-out, in milliseconds

  Note: Specifying a value of less than 10000 reverts to 10000 because 10 seconds is the minimum override.

- To discover and set up applications in Delivery Groups, make sure that there are some machines that are registered and can be powered on. For an App-V application to be discovered, you need to configure App-V Publishing in Studio. [#393676]
- After a user launches the first App-V application, launching a second App-V application too quickly might fail. If this occurs, the user should wait a few minutes so that the initial synchronization can complete, and then launch the second application again. For details about this issue, see CTX138056. [#397521]
- If the antivirus program BitDefender is installed on a VDA, you might not be able to create machine catalogs. There is no workaround for this issue. [#392705]
- After upgrading to XenDesktop 7.5, you cannot create a connection to CloudPlatform or Amazon Web Services (AWS) if the site is configured with a connection to an on-premise hypervisor. You must create a new 7.5 Site. For a hybrid deployment (which includes cloud and non-cloud Sites), you must create separate Sites that share the same StoreFront site.[#454114]
- Creating a machine catalog fails in an environment running VMM 2012 SP1 and Hyper-V 2012 when using a ODX-enabled Storage Area Network. Follow the instructions in http://support.citrix.com/article/CTX139333 to resolve this issue. [#424040]
- The Citrix policy setting **ICA listener connection timeout** applies only to Virtual Delivery Agent 5.0, 5.5, and 5.6 Feature Pack 1, even though the Studio policy editing window says this setting also applies to 7.0 Desktop OS, 7.1 Desktop OS, 7.5 Desktop OS, and 7.6 Desktop OS.
- In Studio, the description of the Citrix policy setting **Launching of non-published programs during client connection** incorrectly states that this setting specified whether to launch initial applications or published applications through ICA or RDP on the server. This setting specifies only whether to launch initial applications or published applications through RDP on the server.

- Citrix policies might not be applied correctly when filtered by tags. To prevent this, apply the hotfix at CTX142439. [#529165]

Director issues

- The User-based application usage data in the Hosted Application Usage reports, is not accurate for time ranges that exceed the last seven days. This occurs because application data beyond the last seven days is deleted. To avoid using incorrect User-based application usage data, only use data reported within the last seven days. [504642]
- Director displays the **Unexpected error. Check your network connection or view server event log for further information** popup error on the Trends and Filters page because the XenDesktop database name includes spaces. The API calls used by Director do not support connecting to a database that has a name containing spaces. Follow database naming requirements when renaming a database. [494339]
- After upgrading, Director does not persist an administrator's UI.GlobalSearchResults settings. To work around this issue, manually edit the UI.GlobalSearchResults setting in the web.config file after upgrading. [484066]
- Hotfix inventory may take several hours to update when large numbers of hotfixes are applied at the same time to environments with more than 20,000 desktops. [#489604]
- Historical information is preserved after you have deleted and then re-created a Delivery Group from the same Session Machine Catalog. The data then incorrectly displays that historical information on the Trends graph and table. To create Delivery Groups without preserving historical trend data, do not re-create the Delivery Group until after you have deleted the machine catalog and created the new catalog. [#480010]
- When navigating from the Filters page to the User Device page, user names may not display. If Delivery Controllers cannot access a domain containing user accounts because of Active Directory restrictions, those full user names may not appear on the User Device page. To work around this issue, ensure that the domain where XenDesktop is installed is trusted by the domain to which the end user belongs. [#479517]
- If all Sites within an existing Site Group do not have assigned delegated administrators, the search for machines and end-point devices within the Site Group fails. To allow an administrator to search across all Sites within a Site Group, add the administrator to the Delegated Administrator group that has permissions to the Sites. [#491740]
- When monitoring Windows XP virtual desktops running WinRM 2.0 for users with VDAs earlier than 7, you must change the WinRM port listening order. For details about how to change the setting to 5985,80, see Advanced configuration. [#273609]
- You cannot edit an existing Site Group using the Director Configuration Tool. To work around this issue, open the .xml configuration file from within the Director Configuration folder, and then modify the Site Group setting. [#491681]
- Using Active Directory Users and Computers to configure users with logon scripts fails and data does not appear in the Logon Duration panel. Instead, to configure users with logon scripts, you must use a Group Policy. [#393259]
- The logon duration data from a first-time logon to a Personal vDisk VDA might not be collected or displayed in Director. For subsequent logons, data appears normally. [#383941]
- When you run a console session from a Windows Server 2012 desktop, navigating to the user details page in Director might result in an error and no data will be displayed.

  As a workaround, register the VDA, log off the current session, and log in to the VDA again. [#388513]

- In the Infrastructure panel of the Dashboard page, Director displays “Not Available” for Citrix CloudPlatform-based host connections, Amazon Web Services, Hyper-V, and Microsoft System Center Configuration Manager and does not provide status information. [#449806, #446397]

- Logon duration does not update in Director's Dashboard view if users launch a hosted application. [#386860]

HDX issues

Note: For the latest updates to HDX Flash compatibility, refer to CTX136588.

- Configuring HDX MediaStream redirection on a new machine fails. To work around this issue, reboot the end-point machine after installing Receiver. [#494741]
- Sessions fail if using a certificate with the SHA512 algorithm for an SSL/TLS connection. This occurs when using Receiver for HTML5 to launch sessions with Server OS machines running Windows Server 2012 R2. To avoid this issue, do not use the SHA512 algorithm for an SSL/TLS certificate in this type of configuration. [#487284]
- With GPU pass-through and NVIDIA Kepler cards, the first connection attempt may fail for a HDX 3D Pro user device with three or four monitors. If this happens, attempt to connect again. [#422049]
- When a user attempts to connect, change the screen resolution, or change the size of the session screen, the screen may flicker or display as black. This may occur if larger resolutions are selected and the video driver cannot allocate enough memory at boot time to support the resolution. You can view the current resolution setting in the session window by selecting Advanced Settings from the Screen Resolution dialog. To allow the driver to allocate enough memory to support higher resolutions, increase the amount of memory for the VDA. Use the following as guidelines: Windows 7: Sum-of-all-monitors (width x height x 4 BytesPerPixel x 2 BackBuffers) Win8: Sum-of-all-monitors (width x height x 4 BytesPerPixel x 3 BackBuffers). [#494671]
- If the USB Redirection policy is enabled, USB storage and audio devices do not work when the user chooses to redirect their devices. This only occurs on Server OS machines running Windows 2012 and later. To exclude audio and storage devices from the list of devices, use the Client USB Device Redirection Rule policy. For additional information on USB redirection rules and configurations, see http://support.citrix.com/article/CTX137939. [#479578]
- When the user attempts to launch a session from a Server OS machine, Receiver displays the "The connection to <app name/desktop name> failed with status (1030)" error message on the user's device after the Session Reliability Connections policy is changed from disabled to enabled by the administrator. To work around this issue, the administrator must restart the VDA for the policy to take effect. [#486073]
- When using Remote PC to run a Lync 2013 session remotely, attached web cameras on client devices are not listed in Lync 2013 in the user's session. To work around this issue, the user can use Device Manager to disable the web cameras on their remote machines. [#482807]
- Even though webcams might support H.264 compression, this release does not support hardware compression, so you must use software compression for those webcams. To do this, add a registry entry on user devices at HKEY_CURRENT_USER\Software\Citrix\HdxRealTime; add a DWORD registry name DeepCompress_ForceSWEncode. When set to 1, software compression is used. By default, this setting is off and hardware compression is used . [#357356]
- HDX RealTime Webcam video lags if the video resolution is higher than 720p (1280x720). [#350187]
- When using HDX Flash Redirection continuously, the session might become unresponsive. [#350085, 361926]
- HDX RealTime Webcam supports most raw formats supported by a webcam, but in rare cases, if the webcam has an unsupported format, that webcam might not work as the Citrix HDX Webcam. [#338318]
- Multiple duplicate images might be seen intermittently when using Citrix HDX Webcam with some models of webcams. [#367322]
- HDX RealTime Webcams are not supported for these applications:
  - Citrix GoToMeeting when hosted on Server OS Machines with Windows 2012 operating systems. [#346430]
  - GoToMeeting (on any platform) if the webcam is attached after a meeting has started. [#346140]
  - Microsoft Lync 2013 and Adobe Connect with VDAs on Windows 8, Windows 8.1, and Windows 2012 operating systems. [#340784, 348506, 459732]
  - Microsoft Office Communications Server (OCS) video calls if the Webcam is attached after the call is in progress. [#370236]
  - Microsoft Silverlight. This is an intermittent issue. As a workaround, on the user device, enable the legacy codec by adding a DWORD registry key value name EnableDeepcompress_Client at HKEY_CURRENT_USER\Software\Citrix\HdxRealTime and setting it to 0. [#379779]
  - 64-bit video conferencing applications. Video compression for 64-bit applications is not supported. [#366515]
- When using HDX 3D Pro with the XenDesktop 5.6 Feature Pack 1 Virtual Desktop Agent on Windows XP virtual desktops, during the first connection, the Fine Drawing (2D) check box is selected and sometimes greyed out. This is due to delayed registry updates, which cause the Config tool UI to pick up incorrect default values during initialization. [#353031]
  As a workaround, disconnect and reconnect the session.

  If the problem persists, clear previous session information by deleting settings under the following registry entry:

HKey_Current_Users\Software\Citrix\HDX3D\BitmapRemotingConfig

- On Windows XP, Citrix HDX webcam might not be detected. As a workaround, install Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package from http://www.microsoft.com/en-us/download/details.aspx?id=14431 website and try again. [#382733]
- When viewing the Display Adapters node from the Device Manager console applet, the Standard VGA Graphics Adapter appears in the list with a yellow exclamation point (yellow bang). You can ignore this warning because it does not affect functionality. This warning occurs because a legacy model XPDM display driver (Standard VGA Graphics Adapter) is not allowed to load when a new model WDDM display driver (Citrix Display Driver) is installed. [#339390]
- Users might experience issues when attempting to play media files on Windows 8 user devices. This is because this product fails to register the correct default program for client-side content fetching protocols used to stream media files to user devices. As a workaround for Microsoft Media Streaming (MMS) and Real Time Streaming (RTS) protocols, change the default program used for playing media files from Windows Media Player to Citrix CSF Handler. There is no workaround for the Hypertext Transfer Protocol (HTTP). [#328805]
- TWAIN redirection fails on hosted shared desktops and applications. This is a third party issue related to TWAIN applications that require TWAIN binaries to be located in certain paths. [#300854, 340999]
  As a workaround, on your Windows Server 2012 machine running the VDA, copy these files to the following locations:
  - Copy "twain_32.dll" to the "\WINDOWS" directory of the User profile (for example, copy twain_32.dll into the folder: "%USERPROFILE%\Windows\").
  - Copy "twain_32.dll.mui" into the "\WINDOWS\en-US\" directory of the User profile (for example, copy twain_32.dll.mui into the folder: "%USERPROFILE%\Windows\en-US\").
- The 64-bit Windows Media Player or QuickTime player cannot play some video files using server-side rendering when HDX MediaStream Windows Media Redirection is disabled. As a workaround, use the 32-bit version of Windows Media Player. [#384759]
- Universal Print Server printers selected in the virtual desktop do not appear in the Devices and Printers window in Windows Control Panel. However, when users are working in applications, they can print using those printers. This issue occurs only on Windows Server 2012, Windows 10 and Windows 8 platforms. [#335153]
- With GPU pass-through and NVIDIA Kepler cards, the first connection attempt may fail for a HDX 3D Pro user device with three or four monitors. The second connection should be successful. [#422049]
- The user's Windows computer stops responding when a GoToMeeting session using a webcam configured for USB redirection is started in a Remote PC Access session with an Intel Core i7 processor-based computer. If this occurs, restart the user's computer and restart the Remote PC Access session. The session resumes where the disconnection occurred. To avoid this occurrence, use HDX webcam video compression instead of USB redirection. For details, see http://support.citrix.com/proddocs/topic/xendesktop-7/hd-new-graphics-video.html. [#423284]
- User devices running Receiver for HTML5 might be unable to connect to a Server OS machine running Windows Server 2012 R2. To avoid this issue:
  - Use an existing machine, rather than a machine created with Machine Creation Services (MCS) or Provisioning Services, as the Windows Server OS machine.
  - If you plan to use machines created with MCS, on the master image for the catalog, edit registry and create the following DWORD value:
    Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.
    HKEY_LOCAL_MACHINE\Software\Citrix\GroupPolicy\Defaults\IcaPolicies\AcceptWebSocketsConnections = 1
    HKEY_LOCAL_MACHINE\Software\Citrix\GroupPolicy\Defaults\IcaPolicies\AllowDesktopLaunchForNonAdmins = 1
    HKEY_LOCAL_MACHINE\Software\Citrix\GroupPolicy\Defaults\IcaPolicies\WebSocketsPort = 8008
    Because the WebSockets port number is set by editing the registry, it is not necessary to enable the Websockets connections Citrix policy for the catalog.
  - If you are using a machine created with Provisioning Services, follow the recommendations in CTX139265. [#424064]
- When HDX Flash Redirection is used with a dual-monitor setup and the Flash content window in full-screen on one monitor, clicking anywhere else on the screen might cause the Flash content window to lose focus and be hidden behind the session window. This is behavior is as designed for HDX Flash Redirection. If this happens, users can make the Flash content window visible again by changing the session window from full-screen mode to window mode using the Citrix Desktop Viewer toolbar. [#567132]

Licensing issues

- Errors may occur when installing the Delivery Controller if the most recent version of the license server is not installed. When upgrading to version 7.6, install the latest version of the License Server before installing any other core components. [#510425]
- When licensing is uninstalled and then reinstalled and a read-only product administrator attempts to view Licensing information in Studio, Studio displays the error "You do not have permissions to perform this operation." A read-only administrator does not have the permission to trust a new License Server. As a workaround, a full license administrator must go to the Licensing node and authenticate the License Server. [#380982]
- If you installed the License Server without successfully configuring it (with the post installation License Server Configuration tool), any subsequent License Server upgrade fails. As a workaround, ensure that every License Server installation is configured with the post-installation License Server Configuration tool. [#377079]
- When you try to start the License Administration Console or the Simple License Service, a blank page might display if the Internet Explorer Enhanced Security Configuration is enabled and the License Administration Console or the Simple License Service is not in the Trusted Sites zone. Workaround: Disable Internet Explorer Enhanced Security Configuration. [#382429]
- If port 8083 is in use when you install or upgrade the product, the License Server configuration and installation fail with a License Server Configuration Failed error. As a workaround, check the event log to ensure the error is actually "Port in use." If it is:
  1. Uninstall the License Server by double-clicking on the CTX_Licensing.msi in the x64\Licensing folder on the product installation media.
  2. Run the installer again. It displays some components as Partially installed. Click Install and the installer completes the installation and configures any necessary product components.
  3. Manually install the License Server and specify port numbers that do not conflict with other applications on the machine. [#390815]
- The user list for the License Administration Console and the Citrix Simple License Service Web page does not support non-ASCII characters in user/group names. Due to this limitation, on a Russian operating system, the BUILTIN Administrators group is not added to the user list because it is created with non-ASCII characters. This issue applies to both fresh installs and upgrades. Any users belonging to the BUILTIN Administrators group in an earlier release of XenDesktop and the Simple License Service will not have access to the License Administration Console or the Simple License Service after an upgrade.
  As a workaround, add ASCII-character versions of Russian users/groups names post-installation using the License Administration Console interface. Alternatively, install the license server on one of the other supported operating systems. [#395305]
- When you install or upgrade the product and have Perpetual (permanent) licenses, Studio might display your licenses with an expiration date of 01/01/2000. You can ignore this expiration date and launch your desktops and applications. [#402975]

Local App Access issues

- In a Windows 8 or Windows Server 2012 hosting environment, if Local App Access is enabled and the extension for a client hosted app does not have a File Type Association (FTA), FTA redirection fails. The user is prompted to select "Look for an app in the Store" or "More options." [#372834]
  As a workaround, use one of these methods on the VDA master image:
  - Rename the DelegateExecute registry value for HKEY_CLASSES_ROOT\Unknown\shell\openas\command\DelegateExecute.
  - Use Notepad to open a file with the extension. FTA redirection will work for subsequent attempts.
- URL redirection is disabled, by default, by Microsoft on Windows Server 2012. To enable it, disable Internet Explorer enhanced configuration mode. [#356260]
- Changes to Local App Access properties during a session do not take effect automatically. As a workaround, log off and log back on. [#357488]
- If Local App Access applications are launched on Windows 8 or Windows 2012 platforms, those VDAs cannot be launched from the Modern shell. As a workaround, close the local application and

then launch the VDA application. [#359670]

- Shellhook.dll is not loaded with Receiver for Windows 3.4 and earlier when local applications are launched. As a workaround, change the value of the registry key LocalAppInit_DLLs to 1 under HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows. If the workaround is not used, client to server FTA redirection does not work correctly. [#356130]
- URL redirection might fail for Internet sites that have a pop-up blocker enabled. As a workaround, disable the pop-up blocker. However, for security reasons, disabling pop-up blocker is not recommended. [#371220]
- When Aero mode is enabled for a VDA session, there are inconsistencies between the VDA local applications and the client-hosted applications (for example, ALT+Tab; flashing taskbar entries, jump list, live preview). For compatibility, disable the Aero mode. [#361043]
- Flash Redirection has compatibility issues such as a WMP black screen and flash pseudo-container window out of bounds. As a workaround, disable Flash redirection. [#360182]
- The Desktop Composition Redirection graphics feature is disabled when Local App Access is enabled. To use that feature, disable Local App Access. [#377386]
- With Session Reliability and Local App Access enabled, if network connectivity is disrupted after you click Home in the product toolbar and display the client's desktop, the VDA session might not display the last screen shown before the network disruption. Instead, only the product toolbar and the client's desktop appear. On the toolbar, only the Disconnect option works. [#357769]
- When Local App Access is enabled and a user changes the product session to full screen before or while playing a media file, some or all of the image does not appear. To work around this issue, relaunch the session. [#402702]

Desktop Lock issues

- After installing Citrix Desktop Lock on a domain-joined Windows 8 machine and restarting it, the desktop background may become black and a My Computer window may be displayed instead of the usual Start screen. To log off the machine, type logoff in the address bar of the window, and press Enter. For more information about configuring Windows 8 machines with Desktop Lock, see Desktop Lock. [#329075]
- If a Windows 8 or Windows 7 machine fails and the user attempts to restart it by pressing Ctrl+Alt+Del, the Windows Security dialog on the local desktop opens. This issue occurs even when the Citrix Desktop Lock software is installed and configured. To resolve this issue, select Start Task Manager to display the Restart dialog. [#337507]
- The Citrix Desktop Lock does not redirect Adobe Flash content to domain-joined user devices. The content can be viewed but is rendered on the server, not locally. As a workaround, configure Adobe Flash redirection for server-side content fetching to pass the content from the server to the user device. This issue does not occur on non-domain-joined devices or when the content is viewed with the Desktop Viewer. [#263092]
- Failure to start the virtual desktop agent (VDA) on the user device may occur if the device is running Windows 7 with Desktop Lock and Receiver for Windows Enterprise 3.4. This may occur if the user is or is not connected to the Internet. The error message, "No Internet Connectivity," may appear when this occurs. This is a third party issue with Microsoft. For a potential resolution, see http://technet.microsoft.com/en-us/library/cc766017. [#408642]

End-user and VDA issues

- Handle leaks by wfica32.exe can occur on the user device when playing Windows Media Player files continuously in a Windows 32-bit XP client session. [#378146]
- Disconnect button is not available to users. As a workaround, provide a shortcut to the TSDiscon.exe utility, which is included with the operating system; this will allow them to disconnect from sessions. [#362937]
- The user may continue to have access to the remote PC after attempting to disconnect. This occurs when the user selects the Disconnect command from the Start menu. There is a delay after Disconnect is selected. If the user presses Ctrl+Alt+Del during this delay, the VDA on the remote PC remains available for several minutes before disconnecting. During that time, the VDA on the user device freezes until the remote VDA disconnects. [#322301]
- For VDAs installed on Windows 7 and Windows 8 platforms, two mouse pointers might be visible: one movable and one locked to the UI. This is a third party issue with the NVidia driver. As a workaround, you can disable NVidia GRID technology (formerly known as VGX) by running MontereyEnable.exe -disable -reset, and then restarting the machine. [#307921]
- The Microsoft Desktop Composition feature has a scalability cost for VDAs. For users requiring maximum scalability, Desktop Composition should be disabled by Microsoft policy for any user not using Desktop Composition Redirection. [#386602]
- In certain scenarios, when users attempt to unlock a locked session locally, the session relocks itself repeatedly. This issue might occur if the user unplugs or powers off a keyboard locally connected to a Remote PC Access machine during a remote ICA session. As a workaround, users should relaunch the session remotely, disconnect the session, and then log on again from the console. [#382554]
- For VDAs earlier than 7, users' data might not appear in Director even after you correctly configure Windows Remote Management (WinRM) for these VDAs. If this issue occurs, restart the WinRM service and the data should display in Director as expected. [#392047]
- In secure environments, a new VDA might fail to register with a Controller. Specifically, when installing a VDA containing a local security policy setting that allows only administrators to access a computer from the network, the VDA installs but cannot register with a Controller. Instead, a warning is issued that user access rights are not properly configured. For more information, see CTX117248. [#336203]
- Receiver for Windows users cannot log on to stores using pass-through authentication, even though the domain pass-through authentication method is enabled in the StoreFront authentication service. To resolve this issue, run the command Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True from a Windows PowerShell command prompt on the Controller. [#330775]
- ICA Roundtrip checks are not supported when legacy graphics mode has been specified using a policy for Windows Server 2012 VDAs. There is no workaround for this issue. Note that Windows 8 VDAs do not support legacy mode, so they are not affected by this issue. [#394824]
- With Windows Server 2012 R2 and older Domain Controllers, if you require users to change their password on next login, an error occurs. To work around this problem, remove the Microsoft update KB2883201. [#438725]
- When users connect directly to VDAs using RDP, the Controller sometimes mistakenly reports additional sessions that do not exist, and these non-existent sessions remain in a Connected state in Studio until the VDA is restarted. [#385823]
- When Passthrough Authentication is implemented for Citrix Storefront on FireFox and Chrome browsers, users are prompted for credentials when launching applications. [#441487]
- For Citrix Receiver for Web with a domain pass-through configuration, when a user logs on to a device using Smartcard and then launches a published desktop, the connection may fail. To work around this issue, edit the default ICA file in the store (for example, in `C:\inetpub\wwwroot\Citrix\Store\App_Data\default.ica`), and add the following line to the `[Application]` section:

  ```
  DisableCtrlAltDel=False
  ```
  [#452813]

Personal vDisk issues

To view personal vDisk related known issues, see Personal vDisks.

Provisioning Services issues

To view Provisioning Services issues, see About Provisioning Services 7.0, 7.1, and 7.6

Features not in this release

Sep 29, 2015

The following features are not currently provided or are no longer supported.

- **Launch touch-optimized desktop -** This setting has been disabled for Windows 10 machines. For more information, see Mobile experience policy settings.
- **Secure ICA encryption below 128-bit** - In releases earlier than 7.x, Secure ICA could encrypt client connections for basic, 40-bit, 56-bit, and 128-bit encryption. In 7.x releases, Secure ICA encryption is available only for 128-bit encryption.
- **Legacy printing** - The following printing features are not supported in 7.x releases:
  - Backward compatibility for DOS clients and 16-bit printers, including legacy client printer name.
  - Support for printers connected to Windows 95 and Windows NT operating systems, including enhanced extended printer properties and Win32FavorRetainedSetting.
  - Ability to enable or disable auto-retained and auto-restored printers.
  - DefaultPrnFlag, a registry setting for servers that is used to enable or disable auto-retained and auto-restored printers, which store in user profiles on the server.
- **Secure Gateway** - In releases earlier than 7.x, Secure Gateway was an option to provide secure connections between the server and user devices. NetScaler Gateway is the replacement option for securing external connections.
- **Shadowing users** - In releases earlier than 7.x, administrators set policies to control user-to-user shadowing. In 7.x releases, shadowing end-users is an integrated feature of the Director component, which uses Windows Remote Assistance to allow administrators to shadow and troubleshoot issues for delivered seamless applications and virtual desktops.
- **Power and Capacity Management** - In releases earlier than 7.x, the Power and Capacity Management feature could be used to help reduce power consumption and manage server capacity. The Microsoft Configuration Manager is the replacement tool for this function.
- **Flash v1 Redirection** - Clients that do not support second generation Flash Redirection (including Receiver for Windows earlier than 3.0, Receiver for Linux earlier than 11.100, and Citrix Online Plug-in 12.1) will fall back to server-side rendering for legacy Flash Redirection features. VDAs included with 7.x releases support second generation Flash Redirection features.
- **Local Text Echo** - This feature was used with earlier Windows application technologies to accelerate the display of input text on user devices on high latency connections. It is not included in 7.x releases due to improvements to the graphics subsystem and HDX SuperCodec.
- **Smart Auditor** - In releases earlier than 7.x, Smart Auditor allowed you to record on-screen activity of a user's session. This component is not available in 7.x releases. In 7.6 Feature Pack 1, it is replaced by Session Recording.
- **Single Sign-on** - This feature, which provides password security, is not supported for Windows 8 and Windows Server 2012 environments. It is still supported for Windows 2008 R2 and Windows 7 environments, but is not included with 7.x releases. You can locate it on the Citrix download website: http://citrix.com/downloads.
- **Oracle database support** - 7.x releases require a SQL Server database.
- **Health Monitoring and Recovery (HMR)** - In releases earlier than 7.x, HMR could run tests on the servers in a server farm to monitor their state and discover any health risks. In 7.x releases, Director offers a centralized view of system health by presenting monitoring and alerting for the entire infrastructure from within the Director console.
- **Custom ICA files** - Custom ICA files were used to enable direct connection from user devices (with the ICA file) to a specific machine. In 7.x releases, this feature is disabled by default, but can be enabled for normal usage using a local group or can be used in high-availability mode if the Controller becomes unavailable.
- **Management Pack for System Center Operations Manager (SCOM) 2007** - The management pack, which monitored the activity of farms using SCOM, does not support 7.x releases.

- **CNAME function** - The CNAME function was enabled by default in releases earlier than 7.x. Deployments depending on CNAME records for FQDN rerouting and the use of NETBIOS names might fail. In 7.x releases, Delivery Controller auto-update is the replacement feature that dynamically updates the list of Controllers and automatically notifies VDAs when Controllers are added to and removed from the Site. The Controller auto-update feature is enabled by default in Citrix policies, but can be disabled by creating a policy.
  Alternatively, you can re-enable the CNAME function in the registry to continue with your existing deployment and allow FQDN rerouting and the use of NETBIOS names. For more information, see CTX137960.

- **Quick Deploy wizard** - In Studio releases earlier than 7.x, this option allowed a fast deployment of a fully installed XenDesktop deployment. The new simplified installation and configuration workflow in 7.x releases eliminates the need for the Quick Deploy wizard option.
- **Remote PC Service configuration file and PowerShell script for automatic administration** - Remote PC is now integrated into Studio and the Controller.
- **Workflow Studio** - In releases earlier than 7.x, Workflow Studio was the graphical interface for workflow composition for XenDesktop. The feature is not supported in 7.x releases.
- **Color depth** - In Studio releases earlier than 7.6, this option in the Delivery group User Setting page set the color depth for a Delivery group. In version 7.6, Delivery group color depth can be set using the New-BrokerDesktopGroup or Set-BrokerDesktopGroup PowerShell cmdlet.
- **Launching of non-published programs during client connection** - In releases earlier than 7.x, this Citrix policy setting specified whether to launch initial applications or published applications through ICA or RDP on the server. In 7.x releases, this setting specifies only whether to launch initial applications or published applications through RDP on the server.
- **Desktop launches** - In releases earlier than 7.x, this Citrix policy setting specified whether non-administrative users can connect to a desktop session. In 7.x releases, non-administrative users must be in a VDA machine's Direct Access Users group to connect to sessions on that VDA. The **Desktop launches** setting enables non-administrative users in a VDA's Direct Access Users group to connect to the VDA using an ICA connection. The **Desktop launches** setting has no effect on RDP connections; users an VDA's Direct Access Users group can connect to the VDA using an RDP connection whether or not this setting is enabled.

Features not in Receiver or that have different default values

- **COM Port Mapping** — COM Port Mapping allowed or prevented access to COM ports on the user device. COM Port Mapping was previously enabled by default. In 7.x releases of XenDesktop and XenApp, COM Port Mapping is disabled by default. For details, see Configure COM Port and LPT Port Redirection settings using the registry.
- **LPT Port Mapping** — LPT Port Mapping controls the access of legacy applications to LPT ports. LPT Port Mapping was previously enabled by default. In 7.x releases, LPT Port Mapping is disabled by default.
- **PCM Audio Codec** — Only HTML5 clients support the PCM Audio Codec in 7.x releases.
- **Support for Microsoft ActiveSync.**
- **Proxy Support for Older Versions** — This includes:
  - Microsoft Internet Security and Acceleration (ISA) 2006 (Windows Server 2003).
  - Oracle iPlanet Proxy Server 4.0.14 (Windows Server 2003).
  - Squid Proxy Server 3.1.14 (Ubuntu Linux Server 11.10).

System requirements

Aug 03, 2016

In this article:

The system requirements in this document were valid when this product version released. System requirements components not covered here (such as StoreFront, host systems, receivers and plug-ins, and Provisioning Services) are described in their respective documentation.

Important: Review Prepare to install before beginning an installation.
Unless otherwise noted, the component installer deploys software prerequisites automatically (such as .NET and C++ packages) if they are not detected on the machine. The Citrix installation media also contains some of this prerequisite software.

The installation media contains several third-party components. Before using the Citrix software, check for security updates from the third party, and install them.

The disk space values are estimates only, and are in addition to space needed for the product image, operating system, and other software.

If you install all the core components (Controller with SQL Server Express, Studio, Director, StoreFront, and Licensing) on a single server, you need a minimum of 3 GB of RAM to evaluate the product; more is recommended when running an environment for users. Performance will vary depending on your exact configuration, including the number of users, applications, desktops, and other factors.

Important: After you install XenApp on a Windows Server 2012 R2 system, use the Kerberos Enable Tool (XASsonKerb.exe) to ensure the correct operation of Citrix Kerberos authentication. The tool is located Support > Tools > XASsonKerb folder on the installation media; you must have local administrator privileges to use the tool. To ensure correct Kerberos operation, run xassonkerb.exe -install from a command prompt on the server. If you later apply an update that changes the registry location HKLM\System\CurrentControlSet\Control\LSA\OSConfig, run the command again. To see all available tool options, run the command with the -help parameter.

Session Recording - XenApp 7.6 FP1, FP2, and LTSR

Session Recording is available in English, French, German, Japanese, Spanish, and simplified Chinese. All Session Recording components that connect to each other must be the same language edition; mixed-language installations are not supported.

The English-language edition of Session Recording is supported on English, Russian, traditional Chinese, and Korean operating systems. The French, German, Japanese, Spanish, and simplified Chinese editions of Session Recording are supported on operating systems in their respective languages.

Feature Pack 1

Session Recording Administration components

You can install the Session Recording Administration components (Session Recording Database, Session Recording Server, and Session Recording Policy Console) on a single server or on separate servers.

Session Recording Database

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

- Microsoft SQL Server 2008 R2 SP3 Shared Management Objects and Microsoft SQL Server 2008 R2 SP3 System CLR Types packages. You can download the packages at http://www.microsoft.com/en-us/download/details.aspx?id=44272.
- Microsoft SQL Server 2014 (Enterprise and Express editions), Microsoft SQL Server 2012 (Enterprise and Express editions) with Service Pack 2, or Microsoft SQL Server 2008 R2 (Enterprise and Express editions) with Service Pack 3
- .NET Framework Version 3.5 Service Pack 1
- .NET Framework Version 3.5 Service Pack 1

Session Recording Server

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

Before starting the Session Recording installation, you must install some prerequisites. Open the Server Manager and add the IIS role. Select the following options:

- Application Development -
  ASP.NET 3.5 (other components are automatically selected. Click Add to accept required roles)
- Security - Windows Authentication
- Management Tools - IIS 6 Management Compatibility
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility
  - IIS 6 Scripting Tools
  - IIS 6 Management Console
- NET Framework Version 3.5 Service Pack 1
- If the Session Recording Server uses HTTPS as its communications protocol, add a valid certificate. Session Recording uses HTTPS by default, which Citrix recommends.
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.

Session Recording Policy Console

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

- .NET Framework Version 3.5 Service Pack 1

Session Recording Agent

Install the Session Recording Agent on every XenApp and XenDesktop server on which you want to record sessions.

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled
- .NET Framework Version 3.5 Service Pack 1

Session Recording Player

Supported operating systems:

- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 with Service Pack 1

For optimal results, install Session Recording Player on a workstation with:

- Screen resolution of 1024 x 768
- Color depth of at least 32-bit
- Memory: 1GB RAM (minimum). Additional RAM and CPU/GPU resources can improve performance when playing graphics intensive recordings; especially when there are a lot of animations in the recordings.

The seek response time depends on the size of the recording and your machine's hardware specification.

Requirements:

- .NET Framework Version 3.5 Service Pack 1

Feature Pack 2 and LTSR

Session Recording Administration components

You can install the Session Recording Administration components (Session Recording Database, Session Recording Server, and Session Recording Policy Console) on a single server or on separate servers.

Session Recording Database

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

- .NET Framework Version 3.5 Service Pack 1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.1 or 4.6.

Session Recording Server

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

Before starting the Session Recording installation, you must install some prerequisites. Open the Server Manager and add the IIS role. Select the following options:

- Application Development:
  - ASP.NET 4.5 on Server 2012 and Server 2012 R2, ASP.NET on Server 2008 R2 (other components are automatically selected. Click Add to accept required roles)
- Security - Windows Authentication
- Management Tools - IIS 6 Management Compatibility
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility
  - IIS 6 Scripting Tools
  - IIS 6 Management Console
- NET Framework Version 3.5 Service Pack 1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.1 or 4.6.
- If the Session Recording Server uses HTTPS as its communications protocol, add a valid certificate. Session Recording uses HTTPS by default, which Citrix recommends.
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.

Session Recording Policy Console

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

- .NET Framework Version 3.5 Service Pack 1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.1 or 4.6.

Session Recording Agent

Install the Session Recording Agent on every XenApp and XenDesktop server on which you want to record sessions.

Supported Windows operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled
- .NET Framework Version 3.5 Service Pack 1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.1 or 4.6.

Session Recording Player

Supported operating systems:

- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 with Service Pack 1

For optimal results, install Session Recording Player on a workstation with:

- Screen resolution of 1024 x 768
- Color depth of at least 32-bit
- Memory: 1GB RAM (minimum). Additional RAM and CPU/GPU resources can improve performance when playing graphics intensive recordings; especially when there are a lot of animations in the recordings.

The seek response time depends on the size of the recording and your machine's hardware specification.

Requirements:

- .NET Framework Version 3.5 Service Pack 1 or .NET Framework Version 4.5.1 or 4.6.

Delivery Controller

Supported operating systems:
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:
- Disk space: 100 MB. Connection leasing (which is enabled by default) adds to this requirement; sizing depends on the number of users, applications, and mode (RDS or VDI). For example, 100,000 RDS users with 100 recently-used applications require approximately 3 GB of space for connection leases; deployments with more applications may require more space. For dedicated VDI desktops, 40,000 desktops require at least 400-500 MB. In any instance, providing several GBs of additional space is suggested.
- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 only).
- Microsoft .NET Framework 4.5.1 (4.5.2 and 4.6 are also supported).
- Microsoft .NET Framework 4.6.1
- Windows PowerShell 2.0 (included with Windows Server 2008 R2) or 3.0 (included with Windows Server 2012 R2 and Windows Server 2012).
- Visual C++ 2005, 2008 SP1, and 2010 Redistributable packages.

Database

Supported Microsoft SQL Server versions for the Site Configuration Database (which initially includes the Configuration Logging Database and the Monitoring Database):

- SQL Server 2016, Express, Standard, and Enterprise Editions.
- SQL Server 2014 through SP2, Express, Standard, and Enterprise Editions.
- SQL Server 2012 through SP3, Express, Standard, and Enterprise Editions. By default, SQL Server 2012 SP1 Express is installed when installing the Controller, if an existing supported SQL Server installation is not detected.
- SQL Server 2008 R2 SP2 and SP3, Express, Standard, Enterprise, and Datacenter Editions.

The following database features are supported (except for SQL Server Express, which supports only standalone mode):

- SQL Server Clustered Instances
- SQL Server Mirroring
- SQL Server 2012 AlwaysOn Availability Groups

Windows authentication is required for connections between the Controller and the SQL Server database.

For information about the latest supported database versions, see CTX114501.

Studio

Supported operating systems:

- Windows 8.1, Professional and Enterprise Editions
- Windows 8, Professional and Enterprise Editions
- Windows 7 Professional, Enterprise, and Ultimate Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:
- Disk space: 75 MB
- Microsoft .NET Framework 4.6.1
- Microsoft .NET Framework 4.5.1 (4.5.2 and 4.6 are also supported)
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 and Windows 7 only)
- Microsoft Management Console 3.0 (included with all supported operating systems)
- Windows PowerShell 2.0 (included with Windows 7 and Windows Server 2008 R2) or 3.0 (included with Windows 8.1, Windows 8, Windows Server 2012 R2, and Windows Server 2012)

Director

Supported operating systems:
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:
- Disk space: 50 MB.
- Microsoft .NET Framework 4.5.1 (4.5.2 and 4.6 are also supported).
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 only)
- Microsoft Internet Information Services (IIS) 7.0 and ASP.NET 2.0. Ensure that the IIS server role has the Static Content role service installed. If these are not already installed, you are prompted for the Windows Server installation media, then they are installed for you.
- Supported browsers for viewing Director:
  - Internet Explorer 11 and 10.
    Compatibility mode is not supported for Internet Explorer. You must use the recommended browser settings to access Director. When you install Internet Explorer, accept the default to use the recommended security and compatibility settings. If you already installed the browser and chose not to use the recommended settings, go to Tools > Internet Options > Advanced > Reset and follow the instructions.
  - Firefox ESR (Extended Support Release).
  - Chrome.

Virtual Delivery Agent (VDA) for Windows Desktop OS

Supported operating systems:
- Windows 10, Enterprise Edition. This applies to XenApp and XenDesktop 7.6 FP3 VDA Standalone installations using the Standard VDA only. The following are not supported on Windows 10 in 7.6 FP3:
  - HDX 3D Pro
  - GPU acceleration
  - Desktop Composition Redirection
  - Legacy graphics mode

    - Secure Boot
    - Publishing Universal Windows apps using VM Hosted Apps
    - Citrix Profile Management
- Windows 8.1, Professional and Enterprise Editions
- Windows 8, Professional and Enterprise Editions
- Windows 7 SP1, Professional, Enterprise, and Ultimate Editions

To use the Server VDI feature, you can use the command line interface to install a VDA for Windows Desktop OS on a supported server operating system; see Server VDI for guidance.

- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:

- Microsoft .NET Framework 4.6.1
- Microsoft .NET Framework 4.5.1 (4.5.2 and 4.6 are also supported)
- Microsoft .NET Framework 3.5.1 (Windows 7 only)
- Microsoft Visual C++ 2005, 2008, and 2010 Runtimes (32-bit and 64-bit). This applies to XenApp and XenDesktop 7.6, 7.6 FP1 and FP2.
- Microsoft Visual C++ 2008, 2010 and 2013 Runtimes (32-bit and 64-bit). This applies to XenApp and XenDesktop 7.6 FP3 VDA Standalone installations.

Remote PC Access uses this VDA, which you install on physical office PCs.

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features will not be installed and will not work. Do not remove Media Foundation from the machine after installing the Citrix software; otherwise, users will not be able to log on to the machine. On most Windows 8.1, Windows 8, and Windows 7 editions, Media Foundation support is already installed and cannot be removed. However, N editions do not include certain media-related technologies; you can obtain that software from Microsoft or a third party.

During VDA installation, you can choose to install the HDX 3D Pro version of the VDA for Windows Desktop OS. That version is particularly suited for use with DirectX and OpenGL-driven applications and with rich media such as video.

Virtual Delivery Agent (VDA) for Windows Server OS

Supported operating systems:

- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

The installer automatically deploys the following requirements, which are also available on the Citrix installation media in the Support folders:

- Microsoft .NET Framework 4.6.1
- Microsoft .NET Framework 4.5.1 (4.5.2 and 4.6 are also supported)
- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 only)
- Microsoft Visual C++ 2005, 2008, and 2010 Runtimes (32-bit and 64-bit). This applies to XenApp and XenDesktop 7.6, 7.6 FP1 and FP2.

- Microsoft Visual C++ 2008, 2010 and 2013 Runtimes (32-bit and 64-bit). This applies to XenApp and XenDesktop 7.6 FP3 VDA Standalone installations.

The installer automatically installs and enables Remote Desktop Services role services, if they are not already installed and enabled.

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that the Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features will not be installed and will not work. Do not remove Media Foundation from the machine after installing the Citrix software; otherwise, users will not be able to log on to the machine. On most Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 editions, the Media Foundation feature is installed through the Server Manager (for Windows Server 2012 R2 and Windows Server 2012: ServerMediaFoundation; for Windows Server 2008 R2: DesktopExperience). However, N editions do not include certain media-related technologies; you can obtain that software from Microsoft or a third party.

Hosts / virtualization resources

Supported platforms:

- XenServer.
  - XenServer 6.5 SP1
  - XenServer 6.5
  - XenServer 6.2 SP1 plus hotfixes (you must apply SP1 to enable application of future hotfixes)
  - XenServer 6.1
- VMware vSphere - No support is provided for vSphere vCenter Linked Mode operation.
  - VMware vSphere 6.0 Update 1
  - VMware vSphere 6.0
  - VMware vSphere 5.5 Update 3
  - VMware vSphere 5.5 Update 2
  - VMware vSphere 5.5 Update 1
  - VMware vSphere 5.5
  - VMware vSphere 5.1 Update 3
  - VMware vSphere 5.1 Update 2
  - VMware vSphere 5.0 Update 3
  - VMware vSphere 5.0 Update 2
  - VMware vCenter 5.5 / 6 appliance
- System Center Virtual Machine Manager - Includes any version of Hyper-V that can register with the supported System Center Virtual Machine Manager versions.
  - System Center Virtual Machine Manager 2012 R2
  - System Center Virtual Machine Manager 2012 SP1
  - System Center Virtual Machine Manager 2012
- Nutanix Acropolis 4.5 - Several XenApp and XenDesktop features are not available when using this platform; see CTX202032 for details. For more information on the use of the product with Acropolis, see https://portal.nutanix.com/#/page/docs.

You can also deploy this product in the following cloud environments:

- Amazon Web Services (AWS)
  - You can provision applications and desktops on supported Windows server operating systems.
  - SQL Server 2012 Enterprise is not available on AWS.

- AWS does not offer desktop operating system instances.
- The Amazon Relational Database Service (RDS) is not supported.
- See the AWS documentation and Deploy XenApp and XenDesktop 7.5 and 7.6 with Amazon VPC for additional information.

- Citrix CloudPlatform
  - The minimum supported version is 4.2.1 with hotfixes 4.2.1-4.
  - Deployments were tested using XenServer 6.2 (with Service Pack 1 and hotfix XS62ESP1003) and vSphere 5.1 hypervisors.
  - CloudPlatform does not support Hyper-V hypervisors.
  - CloudPlatform 4.3.0.1 supports VMware vSphere 5.5.
  - See the CloudPlatform documentation (including the Release Notes for your CloudPlatform version) and XenApp and XenDesktop concepts and deployment on CloudPlatform for additional support and Linux-based system requirements information.

See CTX131239 for updated hypervisor support information.

The following virtualization resource and storage technology combinations are supported for Machine Creation Services and runtime Active Directory account injection into VMs. Combinations marked with an asterisk (*) are recommended.

Virtualization resource	Local Disks	NFS	Block Storage	Storage Link
XenServer	Yes	Yes *	Yes	No
VMware	Yes (no vMotion or dynamic placement)	Yes *	Yes	No
Hyper-V	Yes	No	Yes * (requires Cluster Shared Volumes)	No

The Remote PC Access Wake on LAN feature requires Microsoft System Center Configuration Manager 2012. See Configuration Manager and Remote PC Access Wake on LAN for details.

Active Directory functional level support

The following functional levels for the Active Directory forest and domain are supported:

- Windows 2000 native (not supported for domain controllers)
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

HDX - Desktop Composition Redirection

The Windows user device or thin client must support or contain:

- DirectX 9
- Pixel Shader 2.0 (supported in hardware)
- 32 bits per pixel

- 1.5 GHz 32-bit or 64-bit processor
- 1 GB RAM
- 128 MB video memory on the graphic card or an integrated graphics processor
  HDX queries the Windows device to verify that it has the required GPU capabilities and automatically reverts to server-side desktop composition if it does not. List the devices with the required GPU capabilities that do not meet the processor speed or RAM specifications in the GPO group for devices excluded from Desktop Composition Redirection.

The minimum available bandwidth is 1.5 Mbps; recommended bandwidth is 5 Mbps. Those values incorporate end-to-end latency.

HDX - Windows Media delivery

The following clients are supported for Windows Media client-side content fetching, Windows Media redirection, and real-time Windows Media multimedia transcoding: Receiver for Windows, Receiver for iOS, and Receiver for Linux.

To use Windows Media client-side content fetching on Windows 8 devices, set the Citrix Multimedia Redirector as a default program: in Control Panel > Programs > Default Programs > Set your default programs, select Citrix Multimedia Redirector and click either Set this program as default or Choose defaults for this program.

GPU transcoding requires an NVIDIA CUDA-enabled GPU with Compute Capability 1.1 or higher; see http://developer.nvidia.com/cuda/cuda-gpus.

HDX - Flash Redirection

The following clients and Adobe Flash Players are supported:

- Receiver for Windows (for second generation Flash Redirection features) - Second generation Flash Redirection features require Adobe Flash Player for Other Browsers, sometimes referred to as an NPAPI (Netscape Plugin Application Programming Interface) Flash Player
- Receiver for Linux (for second generation Flash Redirection features) - Second generation Flash Redirection features require Adobe Flash Player for other Linux or Adobe Flash Player for Ubuntu.
- Citrix Online plug-in 12.1 (for legacy Flash Redirection features) - Legacy Flash Redirection features require Adobe Flash Player for Windows Internet Explorer (sometimes referred to as an ActiveX player).

The major version number of the Flash Player on the user device must be greater than or equal to the major version number of the Flash Player on the server. If an earlier version of the Flash Player is installed on the user device, or if the Flash Player cannot be installed on the user device, Flash content is rendered on the server.

The machines running VDAs require:

- Adobe Flash Player for Windows Internet Explorer (the ActiveX player)
- Internet Explorer versions 7, 8, 9, 10, 11 (in non-Modern UI mode). Flash redirection requires Internet Explorer on the server; with other browsers, Flash content is rendered on the server.
- Protected mode disabled in Internet Explorer (Tools > Internet Options > Security tab > Enable Protected Mode check box cleared). Restart Internet Explorer to effect the change.

HDX 3D Pro

When installing a VDA for Windows Desktop OS, you can choose to install the HDX 3D Pro version.

The physical or virtual machine hosting the application can use GPU Passthrough or Virtual GPU (vGPU):

- GPU Passthrough is available with Citrix XenServer. GPU Passthrough is also available with VMware vSphere and VMware ESX, where it is referred to as virtual Direct Graphics Acceleration (vDGA).

- vGPU is available with Citrix XenServer; see www.citrix.com/go/vGPU (Citrix My Account credentials required).

Citrix recommends that the host computer have at least 4 GB of RAM and four virtual CPUs with a clock speed of 2.3 GHz or higher.

Graphical Processing Unit (GPU):
- For CPU-based compression (including lossless compression), HDX 3D Pro supports any display adapter on the host computer that is compatible with the application being delivered.
- For optimized GPU frame buffer access using the NVIDIA GRID API, HDX 3D Pro requires NVIDIA Quadro cards with the latest NVIDIA drivers. The NVIDIA GRID delivers a high frame rate, resulting in a highly interactive user experience.
- For vGPU using XenServer, HDX 3D Pro requirements include NVIDIA GRID K1 and K2 cards.

User device:
- HDX 3D Pro supports all monitor resolutions that are supported by the GPU on the host computer. However, for optimum performance with the minimum recommended user device and GPU specifications, Citrix recommends a maximum monitor resolution for user devices of 1920 x 1200 pixels for LAN connections, and 1280 x 1024 pixels for WAN connections.
- Citrix recommends that user devices have at least 1 GB of RAM and a CPU with a clock speed of 1.6 GHz or higher. Use of the default deep compression codec, which is required on low-bandwidth connections, requires a more powerful CPU unless the decoding is done in hardware. For optimum performance, Citrix recommends that user devices have at least 2 GB of RAM and a dual-core CPU with a clock speed of 3 GHz or higher.
- For multi-monitor access, Citrix recommends user devices with quad-core CPUs.
- User devices do not need a dedicated GPU to access desktops or applications delivered with HDX 3D Pro.
- Citrix Receiver must be installed.

HDX - Video conferencing requirements for webcam video compression

Supported clients: Citrix Receiver for Windows, Receiver for Mac, and Receiver for Linux.

Supported video conferencing applications:
- Citrix GoToMeeting HDFaces
- Adobe Connect
- Cisco WebEx
- IBM Sametime
- Microsoft Lync 2010 and 2013
- Microsoft Office Communicator
- Google+ Hangouts
- Media Foundation-based video applications on Windows 8.x, Windows Server 2012, and Windows Server 2012 R2
- Skype 6.7. To use Skype on a Windows client, edit the registry on the client and the server:
  - Client registry key HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
    Name: DefaultHeight , Type: REG_DWORD, Data: 240

    Name: DefaultWidth, Type: REG_DWORD, Data: 320
  - Server registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility
    Name: skype.exe, Type: REG_DWORD, Data: Set to 0

Other user device requirements:
- Appropriate hardware to produce sound.
- DirectShow-compatible webcam (use the webcam default settings). Webcams that are hardware encoding-capable

reduces client-side CPU usage.
- Webcam drivers, obtained from the camera manufacturer if possible.

HDX - Other

UDP audio for Multi-Stream ICA is supported on Receiver for Windows and Receiver for Linux 13.

Echo cancellation is supported on Citrix Receiver for Windows.

Universal Print Server Requirements

- Universal Print Server - The Universal Print Server comprises client and server components. The UPClient component is included in the VDA installation. The UPServer component (which you install on each print server where the shared printers reside that you want to provision with the Citrix Universal Print Driver in user sessions) is supported on:
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 32-bit
  - Windows Server 2012 R2 and 2012. This applies to minimum XenApp and XenDesktop 7.6 FP3.
- **XenApp and XenDesktop 7.6 FP3**. The following are prerequisites for installing the UPServer component on the print server:
  - Microsoft Visual Studio 2013 Runtime (both 32-bit and 64-bit)
  - Microsoft .NET Framework 4.5.1
  - CDF_x64.msi for 64-bit platforms or CDF_x86.msi for 32-bit platforms
  - UpsServer_x64.msi for 64-bit platforms or UpsServer_x86.msi for 32-bit platforms

    The UPClient component, which you install on XenApp and XenDesktop hosts that provision session network printers, is compatible with Windows 10 desktops and is part of the VDA installation.

User authentication during printing operations requires the Universal Print Server to be joined to the same domain as the Remote Desktop Services VDA.

Other

- Citrix recommends installing or upgrading to the component software versions provided on the installation media for this release.
  - StoreFront requires 2 GB of memory. See the StoreFront documentation for system requirements. StoreFront 2.6 is the minimum supported version with this release.
  - When using Provisioning Services with this release, the minimum supported Provisioning Services version is 7.0.
  - The Citrix License Server requires 40 MB of disk space. See the licensing documentation for system requirements. Only Citrix License Server for Windows is supported. The minimum supported version is 11.12.1.
- The Microsoft Group Policy Management Console (GPMC) is required if you store Citrix policy information in Active Directory rather than the Site Configuration database. For more information, see the Microsoft documentation.
- By default, the Receiver for Windows is installed when you install a VDA. For system requirements information on other platforms, see the Receiver for Windows documentation.
- The Receiver for Linux and the Receiver for Mac are provided on the product installation media. See their documentation for system requirements.
- When using Access Gateway versions earlier than 10.0 with this release, Windows 8.1 and Windows 8 clients are not supported.
- Desktop Lock - Supported operating systems:
  - Windows 7, including Embedded Edition
  - Windows XP Embedded

- Windows Vista

  User devices must be connected to a local area network (LAN).

  Supported Receiver: Citrix Receiver for Windows Enterprise 3.4 package (minimum).

- Client folder redirection - Supported operating systems:
  - Server: Windows Server 2008 R2 SP1, Windows Server 2012, and Windows Server 2012 R2
  - Client (with latest Citrix Receiver for Windows): Windows 7, Windows 8, and Windows 8.1
- Multiple network interface cards are supported.
- See the App-V article for supported versions.

Technical overview

Sep 29, 2015

XenApp and XenDesktop are virtualization solutions that give IT control of virtual machines, applications, licensing, and security while providing anywhere access for any device.

XenApp and XenDesktop allow:

- End users to run applications and desktops independently of the device's operating system and interface.
- Administrators to manage the network and provide or restrict access from selected devices or from all devices.
- Administrators to manage an entire network from a single data center.

XenApp and XenDesktop share a unified architecture called FlexCast Management Architecture (FMA). FMA's key features are the ability to run multiple versions of XenApp or XenDesktop from a single Site and integrated provisioning.

FMA key components

A typical XenApp or XenDesktop environment consists of a few key technology components, which interact when users connect to applications and desktops, and log data about Site activity.

Citrix Receiver

A software client that is installed on the user device, supplies the connection to the virtual machine via TCP port 80 or 443, and communicates with StoreFront using the StoreFront Service API.

StoreFront

The interface that authenticates users, manages applications and desktops, and hosts the application store. StoreFront communicates with the Delivery Controller using XML.

Delivery Controller

The central management component of a XenApp or XenDesktop Site that consists of services that manage resources, applications, and desktops; and optimize and balance the loads of user connections.

Virtual Delivery Agent (VDA)

An agent that is installed on machines running Windows Server or Windows desktop operating systems that allows these machines and the resources they host to be made available to users. The VDA-installed machines running Windows Server OS allow the machine to host multiple connections for multiple users and are connected to users on one of the following ports:

- TCP port 80 or port 443 if SSL is enabled
- TCP port 2598, if Citrix Gateway Protocol (CGP) is enabled, which enables session reliability
- TCP port 1494 if CGP is disabled or if the user is connecting with a legacy client

Broker Service

A Delivery Controller service that tracks which users are logged in and where, what session resources the users have, and if users need to reconnect to existing applications. The Broker Service executes PowerShell and communicates with the Broker agent over TCP port 80. It does not have the option to use TCP port 443.

Broker agent

An agent that hosts multiple plugins and collects real-time data. The Broker agent is located on the VDA and is connected to the Controller by TCP port 80. It does not have the option to use TCP port 443.

Monitor Service

A Delivery Controller component that collects historical data and puts it in the Site database by default. The Monitor

Service communicates on TCP port 80 or 443.

ICA File/Stack

Bundled user information that is required to connect to the VDA.

Site Database

A Microsoft SQL database that stores data for the Delivery Controller, such as site policies, machine catalogs, and delivery groups.

NetScaler Gateway

A data-access solution that provides secure access inside or outside the LAN's firewall with additional credentials.

Director

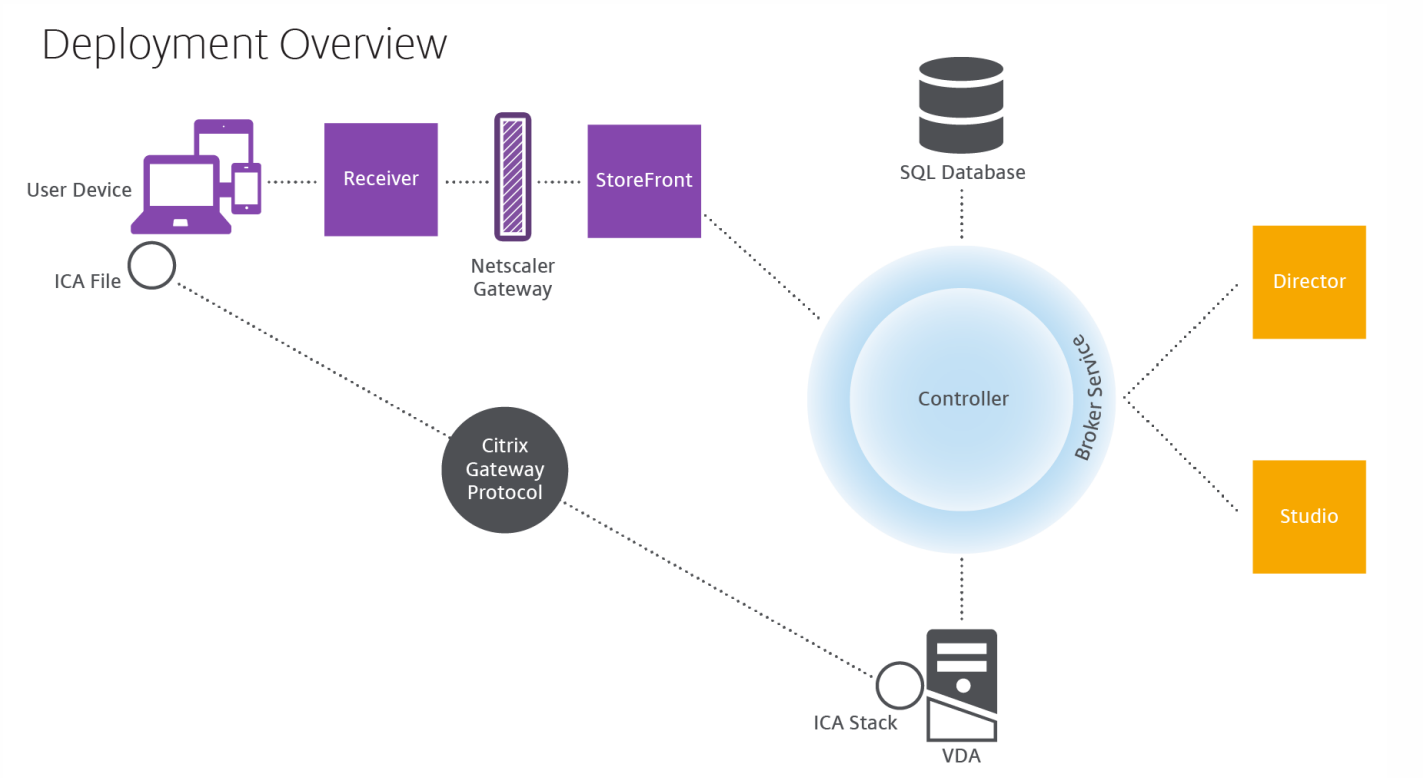
A web-based tool that allows administers access to real-time data from the Broker agent, historical data from the Site database, and HDX data from NetScaler for troubleshooting and support. Director communicates with the Controller on TCP port 80 or 443.

Studio

A management console that allows administers to configure and manage Sites, and gives access to real-time data from the Broker agent. Studio communicates with the Controller on TCP port 80.

How typical deployments work

XenApp and XenDesktop Sites are made up of machines with dedicated roles that allow for scalability, high availability, and failover, and provide a solution that is secure by design. A XenApp or XenDesktop Site consists of VDA-installed Windows servers and desktop machines, and the Delivery Controller, which manages access.



The VDA enables users to connect to desktops and applications. It is installed on server or desktop machines within the data center for most delivery methods, but it can also be installed on physical PCs for Remote PC Access.

The Controller is made up of independent Windows services that manage resources, applications, and desktops, and optimize and balance user connections. Each Site has one or more Controllers, and because sessions are dependent on

latency, bandwidth, and network reliability, all Controllers ideally should be on the same LAN.

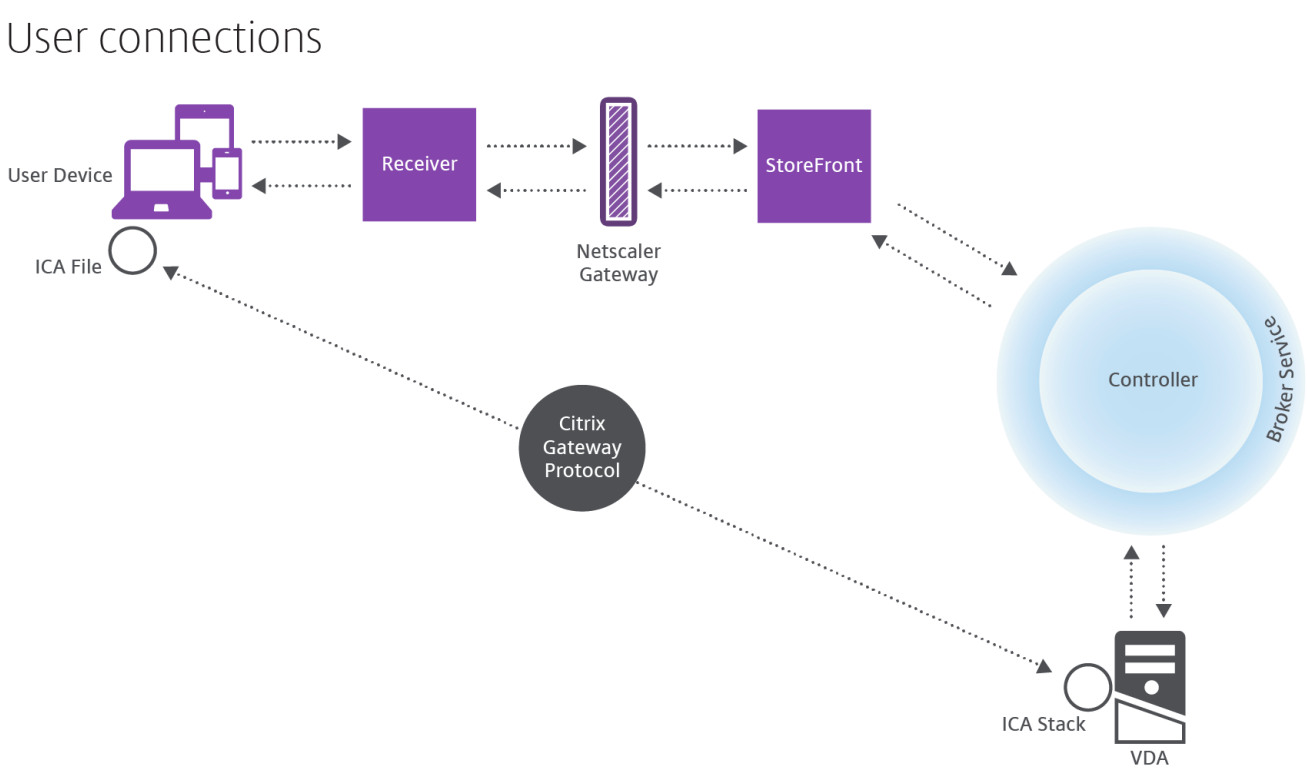
Users never directly access the Controller. The VDA serves as an intermediary between users and the Controller. When users log on to the Site using StoreFront, their credentials are passed through to the Broker Service, which obtains their profiles and available resources based on the policies set for them.

How user connections are handled

To start a XenApp or XenDesktop session, the user connects either via Citrix Receiver, which is installed on the user's device, or via Receiver for Web (RFW).

Within Receiver, the user selects the physical or virtual desktop or virtual application that is needed.

The user's credentials move through this pathway to access the Controller, which determines what resources are needed by communicating with a Broker Service. It is recommended for administrators to put a SSL certificate on StoreFront to encrypt the credentials coming from Receiver.



The Broker Service determines which desktops and applications the user is allowed to access.

Once the credentials are verified, the information about available apps or desktops is sent back to the user through the StoreFront-Receiver pathway. When the user selects applications or desktops from this list, that information goes back down the pathway to the Controller, which determines the proper VDA to host the specific applications or desktop.

The Controller sends a message to the VDA with the user's credentials and sends all the data about the user and the connection to the VDA. The VDA accepts the connection and sends the information back through the same pathways all the way to Receiver. Receiver bundles up all the information that has been generated in the session to create Independent Computing Architecture (ICA). file on the user's device if Receiver is installed locally or on RFW if accessed through the web. As long as the Site was properly set up, the credentials remain encrypted throughout this process.

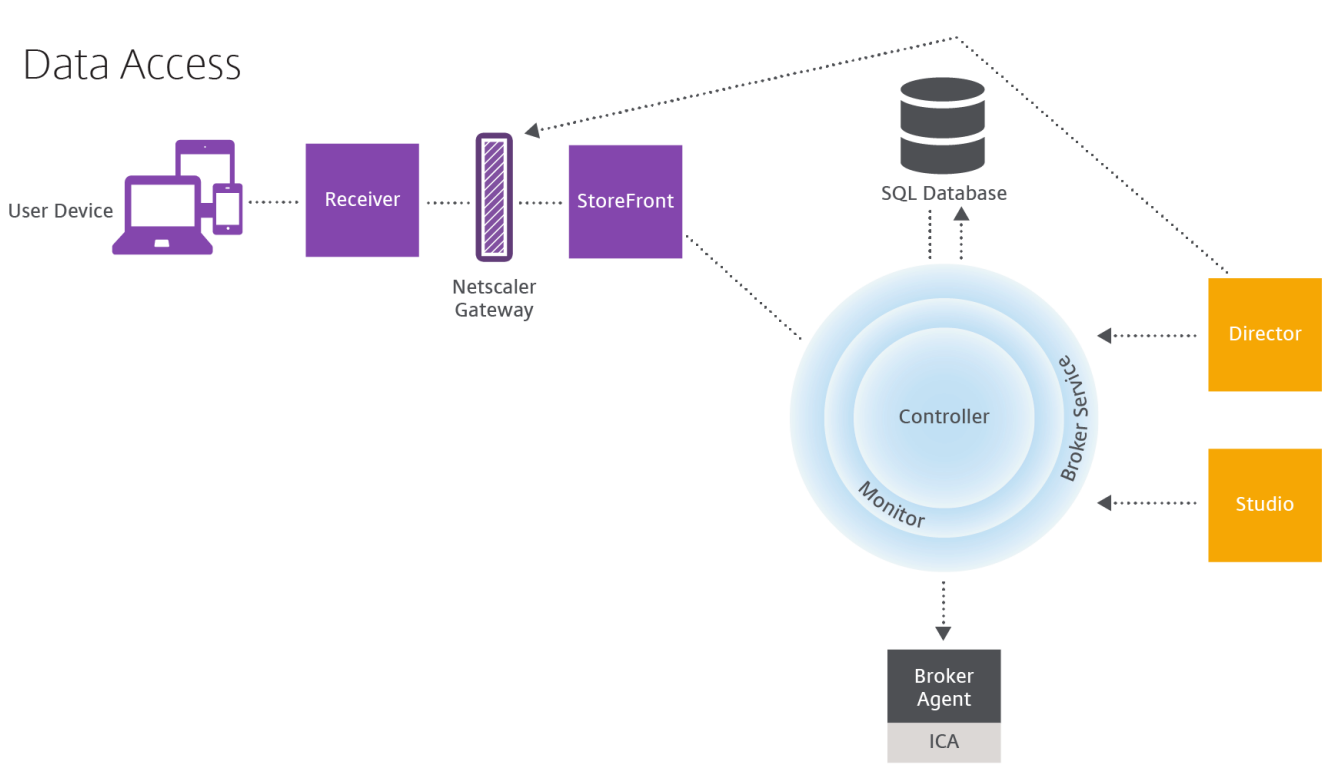
The ICA file is copied to the user's device and establishes a direct connection between the device and the ICA stack running on the VDA. This connection bypasses the management infrastructure: Receiver, StoreFront, and Controller.

The connection between Receiver and the VDA uses the Citrix Gateway Protocol (CGP). If a connection is lost, the Session Reliability feature enables the user to reconnect to the VDA rather than having to relaunch through the management infrastructure. Session Reliability can be enabled or disabled in Studio.

Once the client connects to the VDA, the VDA notifies the Controller that the user is logged on, and the Controller sends this information to the Site database and starts logging data in the Monitoring database.

How data access works

Every XenApp or XenDesktop session produces data that IT can access through Studio or Director. Studio allows administrators to access real-time data from the Broker Agent to better manage sites. Director has access to the same real-time data plus historical data stored in the Monitoring database as well as HDX data from NetScaler Gateway for help-desk support and troubleshooting purposes.



Within the Controller, the Broker Service reports session data for every session on the virtual machine providing real-time data. The Monitor Service also tracks the real-time data and stores it as historical data in the Monitoring database.

Studio can communicate only with the Broker Service; therefore, it has access only to real-time data. Director communicates with the Broker Service (through a plugin in the Broker Agent) to access the Site database.

Director can also access NetScaler Gateway to get information on the HDX data.

Related content

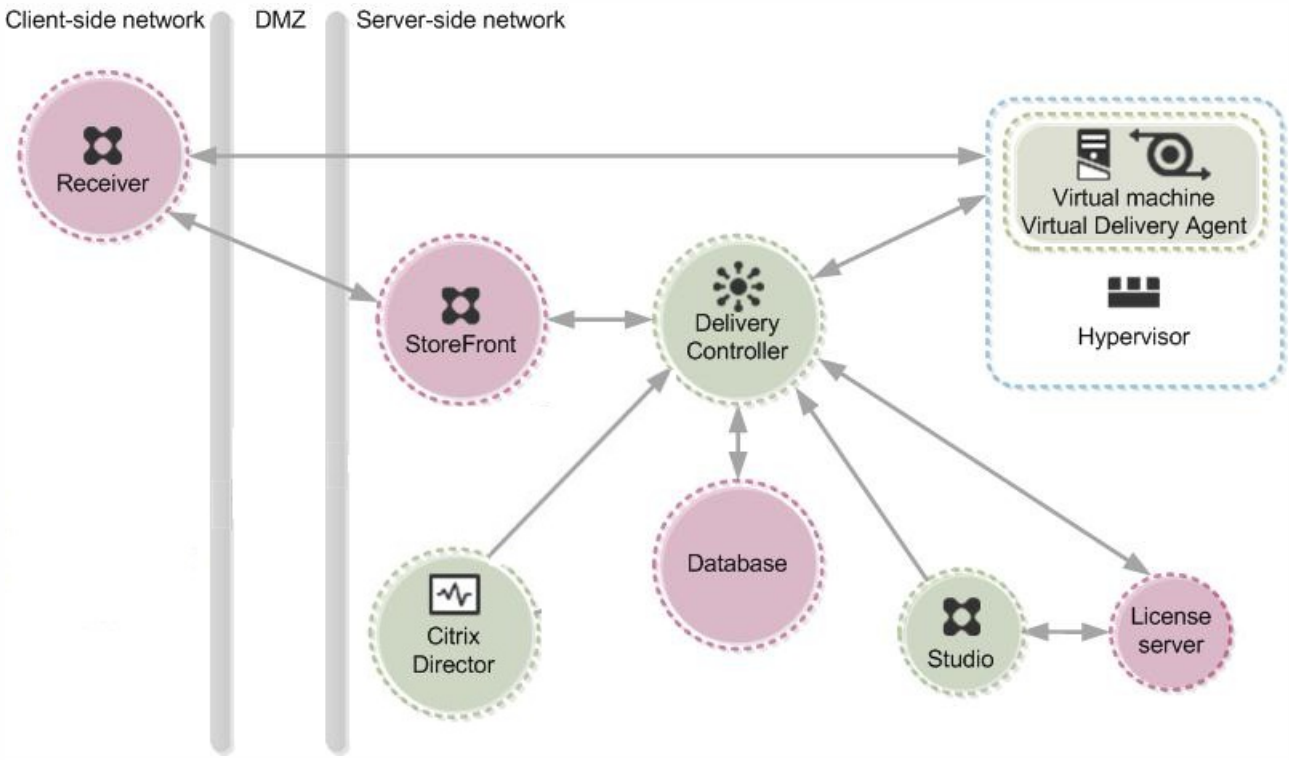
- Concepts and components
- Active Directory

- Fault tolerance
- Delivery methods

Concepts and components

May 11, 2016

This illustration shows the key components in a typical XenApp or XenDesktop deployment, which is called a Site.



The components in this illustration are:

- **Delivery Controller** — The Delivery Controller is the central management component of any XenApp or XenDesktop Site. Each Site has one or more Delivery Controllers. It is installed on at least one server in the data center. (For Site reliability and availability, install the Controller on more than one server.) The Controller consists of services that communicate with the hypervisor to distribute applications and desktops, authenticate and manage user access, broker connections between users and their virtual desktops and applications, optimize use connections, and load-balance these connections.
  Each service's data is stored in the Site database.

  The Controller manages the state of the desktops, starting and stopping them based on demand and administrative configuration. In some editions, the Controller allows you to install Profile management to manage user personalization settings in virtualized or physical Windows environments.

- **Database** — At least one Microsoft SQL Server database is required for every XenApp or XenDesktop Site to store all configuration and session information. This database stores the data collected and managed by the services that make up the Controller. Install the database within your data center, and ensure it has a persistent connection to the Controller.
- **Virtual Delivery Agent (VDA)** — The VDA is installed on each physical or virtual machine in your Site that you want to make available to users. It enables the machine to register with the Controller, which in turn allows the machine and the resources it is hosting to be made available to users. VDAs establish and manage the connection between the machine

and the user device, verify that a Citrix license is available for the user or session, and apply whatever policies have been configured for the session. The VDA communicates session information to the Broker Service in the Controller through the broker agent included in the VDA.
XenApp and XenDesktop include VDAs for Windows server and desktop operating systems. VDAs for Windows server operating systems allow multiple users to connect to the server at one time. VDAs for Windows desktops allow only one user to connect to the desktop at a time.

- **StoreFront** — StoreFront authenticates users to Sites hosting resources and manages stores of desktops and applications that users access. It hosts your enterprise application store, which lets you give users self-service access to desktops and applications you make available to them. It also keeps track of users' application subscriptions, shortcut names, and other data to ensure they have a consistent experience across multiple devices.
- **Receiver** — Installed on user devices and other endpoints, such as virtual desktops, Citrix Receiver provides users with quick, secure, self-service access to documents, applications, and desktops from any of the user's devices, including smartphones, tablets, and PCs. Receiver provides on-demand access to Windows, Web, and Software as a Service (SaaS) applications. For devices that cannot install Receiver software, Receiver for HTML5 provides a connection through a HTML5-compatible web browser.
- **Studio** — Studio is the management console that enables you to configure and manage your deployment, eliminating the need for separate management consoles for managing delivery of applications and desktops. Studio provides various wizards to guide you through the process of setting up your environment, creating your workloads to host applications and desktops, and assigning applications and desktops to users. You can also use Studio to allocate and track Citrix licenses for your Site.
  Studio gets the information it displays from the Broker Service in the Controller.

- **Director** — Director is a web-based tool that enables IT support and help desk teams to monitor an environment, troubleshoot issues before they become system-critical, and perform support tasks for end users. You can use one Director deployment to connect to and monitor multiple XenApp or XenDesktop Sites.
  Director shows session and Site information from these sources:
  - Real-time session data from the Broker Service in the Controller, which include data the Broker Service gets from the broker agent in the VDA.
  - Historical Site data from Monitor Service in the Controller.
  - Data about HDX traffic (also known as ICA traffic) captured by HDX Insight from the NetScaler, if your deployment includes a NetScaler and your XenApp or XenDesktop edition includes HDX Insights.

  You can also view and interact with a user's sessions using Microsoft Remote Assistance.

- **License server** — License server manages your product licenses. It communicates with the Controller to manage licensing for each user's session and with Studio to allocate license files. You must create at least one license server to store and manage your license files.
- **Hypervisor** — The hypervisor hosts the virtual machines in your Site. These can be the virtual machines you use to host applications and desktops as well as virtual machines you use to host the XenApp and XenDesktop components. A hypervisor is installed on a host computer dedicated entirely to running the hypervisor and hosting virtual machines. Citrix XenServer hypervisor is included with XenApp and XenDesktop, but you can use other supported hypervisors, such as Microsoft Hyper-V or VMware vSphere.

  Although most implementations of XenApp and XenDesktop require a hypervisor, you don't need one to provide remote PC access or when you are using Provisioning Services (included with some editions of XenApp and XenDesktop) instead of MCS to provision virtual machine.

These additional components, not shown in the illustration above, may also be included in typical XenApp or XenDesktop deployments:

- **Provisioning Services** — Provisioning Services is an optional component of XenApp and XenDesktop available with some editions. It provides an alternative to MCS for provisioning virtual machines. Whereas MCS creates copies of a master image, Provisioning Services streams the master image to user device. Provisioning Services doesn't require a hypervisor to do this, so you can use it to host physical machines. When Provisioning Services is included in a Site, it communicates with the Controller to provide users with resources.
- **NetScaler Gateway** — When users connect from outside the corporate firewall, this release can use Citrix NetScaler Gateway (formerly Access Gateway) technology to secure these connections with SSL. NetScaler Gateway or NetScaler VPX virtual appliance is an SSL VPN appliance that is deployed in the demilitarized zone (DMZ) to provide a single secure point of access through the corporate firewall.
- **Citrix CloudBridge** — In deployments where virtual desktops are delivered to users at remote locations such as branch offices, Citrix CloudBridge (formerly Citrix Branch Repeater or WANScaler) technology can be employed to optimize performance. Repeaters accelerate performance across wide-area networks, so with Repeaters in the network, users in the branch office experience LAN-like performance over the WAN. CloudBridge can prioritize different parts of the user experience so that, for example, the user experience does not degrade in the branch location when a large file or print job is sent over the network. HDX WAN Optimization with CloudBridge provides tokenized compression and data deduplication, dramatically reducing bandwidth requirements and improving performance. For more information, see the Citrix CloudBridge documentation.

Setting up and assigning resources: machine catalogs and Delivery Groups

With XenApp and XenDesktop, you set up the resources you want to provide to users with machine catalogs, but you designate which users have access to these resources with Delivery Groups.

Machine catalogs

Machine catalogs are collections of virtual or physical machines that you manage as a single entity. These machines, and the application or virtual desktops on them, are the resources you want to provide to your users. All the machines in a machine catalog have the same operating system and the same VDA installed. They also have the same applications or virtual desktops available on them. Typically, you create a master image and use it to create identical virtual machines in the catalog.

When you create a machine catalog, you specify the type of machine and provisioning method for the machines in that catalog.

Machine types

- Windows Server OS machines — Virtual or physical machines based on a Windows server operating system used for delivering XenApp published apps, also known as server-based hosted applications, and XenApp published desktops, also known as server-hosted desktops. These machines allow multiple users to connect to them at one time.
- Desktop OS machines — Virtual or physical machines based on a Windows desktop operating system used for delivering VDI desktops (desktops running Window desktop operating systems that can be fully personalized, depending on the options you choose), and VM-hosted apps (applications from desktop operating systems) and hosted physical desktops. Only one user at a time can connect each of these desktops.
- Remote PC Access — User devices that are included on a whitelist, enabling users to access resources on their office PCs remotely, from any device running Citrix Receiver. Remote PC Access enables you to manage access to office PCs through you XenDesktop deployment.

Provisioning methods

- Machine Creation Services (MCS) — A collection of services that create virtual servers and desktops from a master image

on demand, optimizing storage utilization and providing a virtual machine to users every time they log on. Machine Creation Services is fully integrated and administered in Citrix Studio.

- Provisioning Services — Enables computers to be provisioned and reprovisioned in real-time from a single shared-disk image. Provisioning Services manages target devices as a device collection. The desktop and applications are delivered from a Provisioning Services vDisk that is imaged from a master target device, which enables you to leverage the processing power of physical hardware or virtual machines. Provisioning Services is managed through its own console.
- Existing images — Applies to desktops and applications that you have already migrated to virtual machines in the data center. You must manage target devices on an individual basis or collectively using third-party electronic software distribution (ESD) tools.

Delivery Groups

Delivery Groups are collections of users given to access a common group of resources. Delivery Groups contain machines from your machine catalogs and Active Directory users who have access to your Site. Often it makes sense to assign users to your Delivery Groups by their Active Directory group because both Active Directory groups and Delivery Groups are ways of grouping together users with similar requirements.

Each Delivery Group can contain machines from more than one machine catalog, and each machine catalog can contribute machines to more than one Delivery Group, but each individual machine can only belong to one Delivery Group at a time. You can set up a Delivery Group to deliver applications, desktops, or both.

You define which resources users in the Delivery Group can access. For example, if you want to deliver different applications to different users, one way to do this is to install all the applications you want to deliver on the master image for one machine catalog and create enough machines in that catalog to distribute among several Delivery Groups. Then you configure each Delivery Group to deliver a different subset of the applications installed on the machines.

XenApp and XenDesktop 7.6 differ from XenApp 6.5 and previous versions

If you are familiar with XenApp 6.5 and previous versions of XenApp, it may be helpful to think of XenApp 7.6 and XenDesktop 7.6 in terms of how they differ from those versions.

Although they are not exact equivalents, the following table helps map functional elements from XenApp 6.5 and previous versions to XenApp 7.6 and XenDesktop 7.6:

Instead of this in XenApp 6.5 and before:	**Think of this in XenApp and XenDesktop 7.6:**
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)
Farm	Site
Worker Group	machine catalog Delivery Group
Worker	Virtual Delivery Agent (VDA) Server OS machine, Server OS VDA Desktop OS machine, Desktop OS VDA
Remote Desktop Services (RDS) or Terminal Services machine	Server OS machine, Server OS VDA

Instead of this in XenApp 6.5 and before:	Think of this in XenApp and XenDesktop 7.6:
Zone and Data Collector	Delivery Controller
Delivery Services Console	Citrix Studio and Citrix Director
Publishing applications	Delivering applications
Data store	Database
Load Evaluator	Load Management Policy
Administrator	Delegated Administrator Role Scope

XenApp 7.6 and XenDesktop 7.6 are based on FlexCast Management Architecture (FMA). FMA is a service-oriented architecture that allows interoperability and management modularity across Citrix technologies. FMA provides a platform for application delivery, mobility, services, flexible provisioning, and cloud management.

FMA replaces the Independent Management Architecture (IMA) used in XenApp 6.5 and previous versions.

These are the key elements of FMA in terms of how they relate to elements of XenApp 6.5 and previous versions:

Delivery Sites

Farms were the top-level objects in XenApp 6.5 and previous versions. In XenApp 7.6 and XenDesktop 7.6, the Delivery Site is the highest level item. Sites offer applications and desktops to groups of users.
FMA requires that you must be in a domain to deploy a site. For example, to install the servers, your account must have local administrator privileges and be a domain user in the Active Directory.

Machine catalogs and Delivery Groups

Machines hosting applications in XenApp 6.5 and previous versions belonged to Worker Groups for efficient management of the applications and server software. Administrators could manage all machines in a Worker Group as a single unit for their application management and load-balancing needs. Folders were used to organize applications and machines.
In XenApp 7.6 and XenDesktop 7.6, you use a combination of machine catalogs and Delivery Groups to manage machines, load balancing, and hosted applications or desktops.

Virtual Delivery Agents

In XenApp 6.5 and previous versions, worker machines in Worker Groups ran applications for the user and communicated with data collectors. In XenApp 7.6 and XenDesktop 7.6, the VDA communicates with Delivery Controllers that manage the user connections.

Delivery Controllers

In XenApp 6.5 and previous versions there was a zone master responsible for user connection requests and communication with hypervisors. In XenApp 7.6 and XenDesktop 7.6, Controllers in the Site distribute and handle connection requests. XenApp 6.5 and previous versions, zones provided a way to aggregate servers and replicate data across WAN connections.

Although zones have no exact equivalent in XenApp 7.6 and XenDesktop 7.6, you can provide users with applications that cross WANs and locations. You can design Delivery Sites for a specific geographical location or data center and then allow your users access to multiple Delivery Sites. App Orchestration with XenApp 7.6 and XenDesktop 7.6 provides capabilities for managing multiple Sites in multiple geographies.

Citrix Studio and Citrix Director

Use the Studio console to configure your environments and provide users with access to applications and desktops. Studio replaces the Delivery Services Console in XenApp 6.5 and previous versions.

Administrators use Director to monitor the environment, shadow user devices, and troubleshoot IT issues. To shadow users, Microsoft Remote Assistance must be enabled; it is enabled by default when the VDA is installed.

Delivering applications

XenApp 6.5 and previous versions used the Publish Application wizard to prepare applications and deliver them to users. In XenApp 7.6 and XenDesktop 7.6, you use Studio to create and add applications to make them available to users who are included in a Delivery Group. Using Studio, you first configure a Site, create and specify machine catalogs, and then create Delivery Groups within those machine catalogs. The Delivery Groups determine which users have access to the applications you deliver.

Database

XenApp 7.6 and XenDesktop 7.6 do not use the IMA data store for configuration information. They use a Microsoft SQL Server database to store configuration and session information.

Load Management Policy

In XenApp 6.5 and previous versions, load evaluators use predefined measurements to determine the load on a machine. User connections can be matched to the machines with less load.

In XenApp 7.6 and XenDesktop 7.6, use load management policies for balancing loads across machines.

Delegated Administrators

In XenApp 6.5 and previous versions, you created custom administrators and assigned them permissions based on folders and objects. In XenApp 7.6 and XenDesktop 7.6, custom administrators are based on role and scope pairs. A role represents a job function and has defined permissions associated with it to allow delegation. A scope represents a collection of objects. Built-in administrator roles have specific permissions sets, such as help desk, applications, hosting, and catalog. For example, help desk administrators can work only with individual users on specified sites, while full administrators can monitor the entire deployment and resolve systemwide IT issues.

The transition to FMA also means some features available in XenApp 6.5 and previous versions may be implemented differently or may require you to substitute other features, components, or tools to achieve the same goals.

Instead of this in XenApp 6.5 and before:	Use this in XenApp and XenDesktop 7.6:
Session prelaunch and session linger configured with policy settings	Session prelaunch and session linger configured by editing Delivery Group settings. As in XenApp 6.5, these features help users connect to applications quickly, by starting sessions before they are requested (session prelaunch) and keeping sessions active after a user closes all applications (session linger). In XenApp and XenDesktop 7.6, you enable these features for specified users by configuring these settings for existing Delivery groups. See Configure session prelaunch and session linger.
Support for unauthenticated (anonymous) users provided by granting rights to	Support for unauthenticated (anonymous) users provided by configuring this option when setting user properties of a Delivery Group. See Users.

Instead of this in XenApp 6.5 and before:	Use this in XenApp and XenDesktop 7.6:
anonymous user when setting the properties of published applications	
Local host cache permits a worker servers to function even when a connection to the data store is not available	Connection leasing enables users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available. The connection leasing feature supplements the SQL Server high availability best practices. See Connection leasing.
Application streaming	App-V delivers streamed applications, managed using Studio.
Web Interface	Citrix recommends you transition to StoreFront.
SmartAuditor	Use configuration logging to log all session activities from an administrative perspective or use a third-party, Citrix-ready tool to record sessions.

Active Directory

Apr 27, 2015

Active Directory is required for authentication and authorization. The Kerberos infrastructure in Active Directory is used to guarantee the authenticity and confidentiality of communications with the Delivery Controllers. For information about Kerberos, see the Microsoft documentation.

The System requirements document lists the supported functional levels for the forest and domain. To use Policy Modeling, the domain controller must be running on Windows Server 2003 to Windows Server 2012 R2; this does not affect the domain functional level.

This product supports:

- Deployments in which the user accounts and computer accounts exist in domains in a single Active Directory forest. User and computer accounts can exist in arbitrary domains within a single forest. All domain functional levels and forest functional levels are supported in this type of deployment.
- Deployments in which user accounts exist in an Active Directory forest that is different from the Active Directory forest containing the computer accounts of the controllers and virtual desktops. In this type of deployment, the domains containing the Controller and virtual desktop computer accounts must trust the domains containing user accounts. Forest trusts or external trusts can be used. All domain functional levels and forest functional levels are supported in this type of deployment.
- Deployments in which the computer accounts for Controllers exist in an Active Directory forest that is different from one or more additional Active Directory forests that contain the computer accounts of the virtual desktops. In this type of deployment a bi-directional trust must exist between the domains containing the Controller computer accounts and all domains containing the virtual desktop computer accounts. In this type of deployment, all domains containing Controller or virtual desktop computer accounts must be at "Windows 2000 native" functional level or higher. All forest functional levels are supported.
- Writable domain controllers. Read-only domain controllers are not supported.

Optionally, Virtual Delivery Agents (VDAs) can use information published in Active Directory to determine which Controllers they can register with (discovery). This method is supported primarily for backward compatibility, and is available only if the VDAs are in the same Active Directory forest as the Controllers. For information about this discovery method see Active Directory OU-based Controller discovery and CTX118976.

Deploy in a multiple Active Directory forest environment

Note: This information applies to minimum version XenDesktop 7.1 and XenApp 7.5. It does not apply to earlier versions of XenDesktop or XenApp.
In an Active Directory environment with multiple forests, if one-way or two-way trusts are in place you can use DNS forwarders for name lookup and registration. To allow the appropriate Active Directory users to create computer accounts, use the Delegation of Control wizard. Refer to Microsoft documentation for more information about this wizard.

No reverse DNS zones are necessary in the DNS infrastructure if appropriate DNS forwarders are in place between forests.

The SupportMultipleForest key is necessary if the VDA and Controller are in separate forests, regardless of whether the Active Directory and NetBios names are different. The SupportMultipleForest key is only necessary on the VDA. Use the following information to add the registry key:
Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor

at your own risk. Be sure to back up the registry before you edit it.

- HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest
  - Name: SupportMultipleForest
  - Type: REG_DWORD
  - Data: 0x00000001 (1)

You might need reverse DNS configuration if your DNS namespace is different than that of Active Directory.

If external trusts are in place during setup, the ListOfSIDs registry key is required. The ListOfSIDs registry key is also necessary if the Active Directory FQDN is different than the DNS FQDN or if the domain containing the Domain Controller has a different Netbios name than the Active Directory FQDN. To add the registry key, use the following information:

- For a 32-bit or 64-bit VDA, locate the registry key HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs
  - Name: ListOfSIDs
  - Type: REG_SZ
  - Data: Security Identifier (SID) of the Controllers

When external trusts are in place, make the following changes on the VDA:

1. Locate the file <ProgramFiles>\Citrix\Virtual Desktop Agent\brokeragentconfig.exe.config.
2. Make a backup copy of the file.
3. Open the file in a text editing program such as Notepad.
4. Locate the text allowNtlm="false" and change the text to allowNtlm="true".
5. Save the file.

After adding the ListOfSIDs registry key and editing the brokeragent.exe.config file, restart the Citrix Desktop Service to apply the changes.

The following table lists the supported trust types:

Trust type	Transitivity	Direction	Supported in this release
Parent and child	Transitive	Two-way	Yes
Tree-root	Transitive	Two-way	Yes
External	Nontransitive	One-way or two-way	Yes
Forest	Transitive	One-way or two-way	Yes
Shortcut	Transitive	One-way or two-way	Yes
Realm	Transitive or nontransitive	One-way or two-way	No

For more information about complex Active Directory environments, see CTX134971.

Fault tolerance

Apr 27, 2015

This document outlines ways in which you can increase the level of fault tolerance in your deployment to make sure that business-critical applications and desktops are always available.

Configure database fault tolerance

All information is stored in the Site configuration database; Delivery Controllers communicate only with the database and not with each other. A Controller can be unplugged or turned off without affecting other Controllers in the Site. This means, however, that the Site configuration database forms a single point of failure. If the database server fails, existing connections to virtual desktops will continue to function until a user either logs off or disconnects from a virtual desktop; new connections cannot be established if the database server is unavailable.

Citrix recommends that you back up the database regularly so that you can restore from the backup if the database server fails. In addition, there are several high availability solutions to consider for ensuring automatic failover:

- SQL Mirroring — This is the recommended solution. Mirroring the database makes sure that, should you lose the active database server, the automatic failover process happens in a matter of seconds, so that users are generally unaffected. This method, however, is more expensive than other solutions because full SQL Server licenses are required on each database server; you cannot use SQL Server Express edition for a mirrored environment.
- Using the hypervisor's high availability features — With this method, you deploy the database as a virtual machine and use your hypervisor's high availability features. This solution is less expensive than mirroring as it uses your existing hypervisor software and you can also use SQL Express. However, the automatic failover process is slower, as it can take time for a new machine to start for the database, which may interrupt the service to users.
- SQL Clustering — The Microsoft SQL clustering technology can be used to automatically allow one server to take over the tasks and responsibilities of another server that has failed. However, setting up this solution is more complicated, and the automatic failover process is typically slower than with alternatives such as SQL Mirroring.
- AlwaysOn Availability Groups is an enterprise-level high-availability and disaster recovery solution introduced in SQL Server 2012 to enable you to maximize availability for one or more user databases. AlwaysOn Availability Groups requires that the SQL Server instances reside on Windows Server Failover Clustering (WSFC) nodes. For more information, see AlwaysOn Availability Groups (SQL Server).

Note: Installing a Controller on a node in an SQL clustering or SQL mirroring installation is not supported.

Configure a Site to use a mirror database

The configuration process involves tasks an administrator completes using SQL Server management tools before creating the Site. The remaining tasks occur when the administrator runs the Site creation wizard.

A mirror environment requires at least two SQL Server machines (in the following example, SQL Server A and SQL Server B). SQL Server Express edition cannot be used as either a principal or mirror.

Using Microsoft SQL Server management tools, configure the SQL Server databases:

1. Install the SQL Server software on SQL Server A and SQL Server B.
2. On SQL Server A, create the database intended to be used as the principal (for example, myDatabaseMirror).
   - Make sure that the database uses the full recovery model and not the simple model. (The simple model is configured by default, but prevents the transaction log from being backed up.)
   - Use the following collation setting when creating the database: Latin1_General_100_CI_AS_KS (where Latin1_General varies depending on the country; for example Japanese_100_CI_AS_KS). If this collation setting is not

specified during database creation, subsequent creation of the service schemas within the database will fail, and an error similar to "<service>: schema requires a case-insensitive database" appears (where <service> is the name of the service whose schema is being created).
    - Enable a Read-Committed snapshot as described in CTX137161. It is important to enable this before the database is mirrored to avoid errors.
3. On SQL Server A, back up the database to a file and copy it to SQL Server B.
4. On SQL Server B, restore the backup file to that server (SQL Server B).
5. On SQL Server A, start mirroring.

The next step depends on whether the Citrix administrator (that is, the person running the Site creation wizard) also has full database privileges:

- If the Citrix administrator has database privileges (the same person is the database administrator and the Citrix administrator), Studio does everything for you:
    1. The Citrix administrator uses Studio to create a Site, specifying the address of the previously-created SQL Server A database and its name (myDatabaseMirrorForXD).
    2. The database scripts are automatically applied and the principal and mirror databases are set.
- If the Citrix administrator does not have database privileges, the Citrix administrator must get help from a database administrator:
    1. The Citrix administrator uses Studio to create a Site, specifying the address of the previously-created SQL Server and its name (myDatabaseMirrorForXD).
    2. In the Site creation wizard, selecting Generate Script generates a mirror script and a primary script. The Citrix administrator gives those scripts to the database administrator, who applies the scripts (the mirror script should be applied first). The database administrator must tell the Citrix administrator when that task is completed.
    3. Back in Studio, the Citrix administrator can now complete the Create Site wizard. The principal and mirror databases are set.

To verify mirroring after creating the Site, run the PowerShell cmdlet get-configdbconnection to make sure that the Failover Partner has been set in the connection string to the mirror.

If you later add, move, or remove a Delivery Controller in a mirrored database environment, see Add, remove, or move Controllers, or move a VDA for considerations.

Ensure desktop and application access if Controllers fail

If all Delivery Controllers in a Site fail, you can configure the Virtual Delivery Agents to operate in high availability mode so that users can continue to access and use their desktops and applications. In high availability mode, the VDA accepts direct ICA connections from users, rather than connections brokered by the Controller.

This feature is for use only on the rare occasion when communication with all Controllers fails; it is not an alternative to other high availability solutions. For more information, see CTX127564.

When the database is not available

The connection leasing feature supplements the SQL Server high availability best practices by enabling users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available. For details, see Connection leasing.

Delivery methods

Sep 18, 2014

It's challenging to meet the needs of every user with one virtualization deployment. XenApp and XenDesktop allow administrators to customize the user experience with a variety of methods sometimes referred to as FlexCast models.

This collection of delivery methods — each with its own advantages and disadvantages — provide the best user experience in any use-case scenario.

Mobilize Windows applications on mobile devices

Touch-screen devices, such as tablets and smartphones, are now standard in mobility. These devices can cause problems when running Windows-based applications that typically utilize full-size screens and rely on right-click inputs for full functionality.

XenApp with Citrix Receiver offers a secure solution that allows mobile-device users access to all the functionality in their Windows-based apps without the cost of rewriting those apps for native mobile platforms.

The XenApp published apps delivery method utilizes HDX Mobile technology that solves the problems associated with mobilizing Windows applications. This method allows Windows applications to be refactored for a touch experience while maintaining features such as multitouch gestures, native menu controls, camera, and GPS functions. Many touch features are available natively in XenApp and XenDesktop and do not require any application source code changes to activate.

These features include:

- Automatic display of the keyboard when an editable field has the focus
- Larger picker control to replace Windows combo box control
- Multitouch gestures, such as pinch and zoom
- Inertia-sensed scrolling
- Touchpad or direct-cursor navigation

Reduce PC refresh costs

Upgrading physical machines is a daunting task many businesses face every three to five years, especially if the business needs to maintain the most up-to-date operating systems and applications. Growing businesses also face daunting overhead costs of adding new machines to their network.

The VDI Personal vDisk delivery method provides fully personalized desktop operating systems to single users on any machine or thin client using server resources. Administrators can create virtual machines whose resources — such as processing, memory, and storage — are stored in the network's data center.

This can extend the life of older machines, keep software up to date, and minimize downtime during upgrades.

Ensure secure access to virtual apps and desktops for contractors and partners

Network security is an ever-growing problem, especially when working with contractors, partners, and other third-party contingent workers who need access to a company's apps and data. The workers may also need loaner laptops or other devices, which cause additional cost concerns.

Data, applications, and desktops are stored behind the firewall of the secure network with XenDesktop and XenApp, so the only thing the end user transmits is user-device inputs and outputs, such as keystrokes, mouse clicks, audio, and screen

updates. By maintaining these resources in a data center, XenDesktop and XenApp offer a more secure remote access solution than using the typical SSL VPN.

With a VDI with Personal vDisk deployment, administrators can utilize thin clients or users' personal devices by creating a virtual machine on a network server and providing a single-user desktop operating system. This allows IT to maintain security with third-party workers without the need of purchasing expensive equipment.

Accelerate Migration

When switching to a new operating system, IT can face the challenge of delivering legacy and incompatible applications.

With virtual-machine-hosted apps, users can run older applications through Citrix Receiver on the upgraded virtual machine without any compatibility issues. This allows IT additional time to resolve and test application compatibility issues, ease users into the transition, and make help desk calls more efficient.

Additional benefit for using XenDesktop during migration include:

- Reducing complexity for desktops
- Improving IT's control
- Enhancing end-user flexibility in terms of device usage and workspace location

Enable designers and engineers by virtualizing professional 3-D graphics apps

Many design firms and manufacturing companies rely heavily on professional 3-D graphics applications. These companies face financial strain from the costs of powerful hardware to support this type of software and also logistic problems that come with the sharing of large design files via FTP, email, and similar ad hoc methods.

XenDesktop's hosted physical desktop delivery method provides a single desktop image to workstations and blade servers without the need of hypervisors to run graphic-intensive 3-D applications on a native operating system.

All files are saved in a central data center within the network, so sharing large design files to other users in the network is faster and more secure because the files are not being transferred from one workstation to another.

Transform call centers

Businesses that need large-scale call centers face the difficult challenge of maintaining adequate staffing for peak periods while not overprovisioning machines during less busy hours.

The Pooled VDI delivery method provides multiple users access to a standardized desktop dynamically at a minimal cost when provisioning a large number of users. The pooled machines are allocated on a per-session, first-come, first-served basis.

There is less day-to-day management of these virtual machines because any change made during the session is discarded when the user logs off. This also increases security.

The XenApp hosted desktops delivery method is another viable option for transforming call centers. This method hosts multiple user desktops on a single server-based operating system.

This is a more cost-efficient method than Pooled VDI, but with XenApp hosted desktops, users are restricted from installing applications, changing system settings, and restarting the server.

New deployments

Apr 21, 2016

To build a XenApp or XenDesktop deployment:

1. Set up the virtualization environment to host and manage the components of your XenApp or XenDesktop environment. See System requirements for supported versions of the virtualization platforms, management tools, and cloud deployment solutions listed here.

   You can use these virtualization platforms to host and manage machines in your XenApp or XenDesktop environment:
   - XenServer. See XenServer for information on setting up and using XenServer.
   - VMware vSphere. See Prepare the virtualization environment: VMware for guidance on setting up and using VMware vSphere with XenApp or XenDesktop.
   - Hyper-V with Microsoft System Center Virtualization Machine Manager (VMM). See Prepare the virtualization environment: Microsoft System Center Virtual Machine Manager for guidance on setting up and using Hyper-V with VMM with XenApp or XenDesktop.

   You can use Microsoft System Center Configuration Manager with Citrix Connector 7.5 for System Center Configuration Manager 2012 to manage physical and virtual machines in your XenApp or XenDesktop environment or use it to enable the Wake on LAN feature of Remote PC Access. See Prepare for using Microsoft System Center Configuration Manager.

   You can use these cloud deployment solutions to host product components and provision virtual machines. These solutions pool computing resources to build public, private, and hybrid Infrastructure as a Service (Iaas) clouds.

   - Amazon Web Services, see Deploy XenApp and XenDesktop 7.5 and 7.6 with Amazon VPC.
   - Citrix CloudPlatform, see XenApp and XenDesktop concepts and deployment on CloudPlatform.

2. Set up the non-Citrix infrastructure components required to build your XenApp or XenDesktop Site. These include at least one domain controller running Active Directory Domain Services.

3. Install the Citrix components that make up your XenApp or XenDesktop Site. You can install components using a wizard-based graphical interface or a command-line interface, which enables scripted installation. Both methods install most prerequisites automatically.
   1. Before beginning any installation, review the System requirements. Also, read and complete the Prepare to install checklist.
   2. Install the core components: Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server, and Citrix StoreFront. See Install using the graphical interface or Install using the command line for information on installing these components.
   3. From Studio, create a Site. See Create a Site.
   4. Install a Virtual Delivery Agent (VDA), either on the master image you will use to create virtual machines or directly on each machine. See Install using the graphical interface or Install using the command line for information on installing the VDA. You may also want to see Install or remove Virtual Delivery Agents using scripts.
      For Remote PC Access deployments, install a VDA for Desktop OS on each office PC. Citrix recommends using the VDA installer's command line interface and your existing Electronic Software Distribution (ESD) methods.
   5. Optionally, install the Universal Print Server on the print servers in your environment. See Install using the graphical interface or Install using the command line for information on installing the Universal Print Server.

4. Optionally, integrate additional Citrix components into your XenApp or XenDesktop deployment. For example:

- Provisioning Services is an optional component of XenApp and XenDesktop that provisions machines by streaming a master image to target devices. See Provisioning Services.
- Citrix NetScaler Gateway is a secure application access solution that provides administrators granular application-level policy and action controls to secure access to applications and data. See Citrix NetScaler Gateway.
- Citrix CloudBridge is a set of appliances that optimize WAN performance. See Citrix CloudBridge.

5. Set up the resources you will deliver to users. How you do this depends on the delivery method you are using, but this is the basic sequence for most delivery methods:
   1. Using your hypervisor's management tool , create a master image that defines the desktops or applications you want to provide. See Prepare a master image.
   2. Create a machine catalog containing physical and virtual machines from that master image. See Create a machine catalog.
      - If you are using Machine Creation Services to provision machines, you can add machines to the machine catalog from within Studio.
      - If you are using Provisioning Services to provision machines, you add machines to the machine catalog from the Provisioning Services console.
   3. From Studio, create a Delivery Group to specify which users can access these machines and the applications installed on them. See Delivery groups.

Prepare to install

Jul 07, 2016

The following tables list tasks to complete and things to consider or be aware of before installing the core components (Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server, StoreFront) and Virtual Delivery Agents (VDAs).

Core component and general installation preparation

	Description

	First:
	• If you are unfamiliar with the product, review the Technical overview and related content.
	• Check
	— Known issues
	for installation issues you might encounter.
	• If you are installing components in a cloud environment, see:
	  • Deploy XenApp and XenDesktop 7.5 and 7.6 with Amazon VPC for Amazon Web Services;
	  • XenApp and XenDesktop concepts and deployment on CloudPlatform for Citrix CloudPlatform.
	• If you are using XenServer for your virtualization environment, see the XenServer documentation for guidance.
	• If you are using VMware or Microsoft System Center Virtual Machine Manager for your virtualization environment, see the linked documents.

	Decide where you will install the components and then prepare the machines and operating systems.
	• Review System requirements for supported operating systems and versions for the Controller, Studio, Director, Virtualization resources, and VDAs. The Citrix StoreFront and the Citrix License Server requirements documents specify their supported platforms.
	  • You can install the core components on the same server or on different servers. For example, to manage a smaller deployment remotely, you can install Studio on a different machine than the server where you installed the Controller. To accommodate future expansion, consider installing components on separate servers; for example, install the License Server and Director on different servers.
	  • You can install both the Delivery Controller and the Virtual Delivery Agent for Windows Server OS on the same server. Launch the installer and select the Delivery Controller (plus any other core components you want on that machine); then launch the installer again and select the Virtual Delivery Agent for Windows Server OS.
	  • Do not install Studio on a server running XenApp 6.5 Feature Pack 2 for Windows Server 2008 R2 or any earlier version of XenApp.
	• Be sure that each operating system has the latest updates.
	• Be sure that all machines have synchronized system clocks. Synchronization is required by the Kerberos infrastructure that secures communication between the machines.
	• Components are installed in C:\Program Files\Citrix by default. You can specify a different location during installation, but it must have execute permissions for network service.
	• Most component prerequisites are installed automatically; however, the
	— System requirements
	document notes exceptions.

	Decide where to install the SQL Server software for the Site Configuration Database. • By default, SQL Server 2012 Express is installed automatically on the server when you install the Controller, if another instance is not detected. The default installation uses the default Windows service accounts and permissions. Refer to Microsoft documentation for details of these defaults, including the addition of Windows service accounts to the sysadmin role. The Controller uses the Network Service account in this configuration. The Controller does not require any additional SQL Server roles or permissions. If required, you can select **Hide instance** for the database instance. When configuring the address of the database in Studio, enter the instance's static port number, rather than its name. Refer to Microsoft documentation for details about hiding an instance of SQL Server Database Engine.

Description
• Alternatively, you can separately install a supported SQL Server version on that server or on a different server. In such cases, the SQL Server software does not need to be installed before you install the core components, but it must be installed before you create the Site. • Review the database considerations in the *— Plan* documents, and set up any supported redundancy infrastructure. Important: Windows authentication is required between the Controller and the database.
Decide how you want ports opened. By default, the following ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. You can disable this default action and open the ports manually if you use a third-party firewall or no firewall, or if you just prefer to do it yourself. • Controller: TCP 80, 443 • Director: TCP 80, 443 • License Server: TCP 7279, 8082, 8083, 27000 • StoreFront: TCP 80, 443 Tip: For complete port information, see CTX101810. For additional installation options, see Install using the command line.
Configure your Active Directory domain. • In addition to being a domain user, you must be a local administrator on the machines where you are installing core components. • Do not attempt to install any components on a domain controller. • The *— System requirements* document lists the supported functional levels. See the Microsoft documentation for instructions. When you install the License Server, that user account is automatically made a full administrator on the license server.
Before you install Director, decide if you will use the shadowing feature of Director, which uses Windows Remote Assistance.
Good to know: • If a component does not install successfully, the process stops with an error message. Components that installed successfully are retained; you do not need to reinstall them. • Studio starts automatically after it is installed. You can disable this action during installation. • When you create objects before, during, and after installation, it is best practice to specify unique names for each object (for example networks, groups, catalogs, resources). • After installing components in Amazon Web Services (AWS), you will need to know the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials when you use Studio to create a Site.

VDA installation preparation

Description
If you will be installing a VDA for Windows Desktop OS, decide if you want to install the HDX 3D Pro version. The HDX3D Pro feature delivers desktops and applications that perform best with a GPU for hardware acceleration. For more information, see the HDX 3D Pro documentation.
Decide how you will use the VDA. The default setting assumes that you will use a master image containing an installed VDA with Machine Creation Services or Provisioning Services to create other virtual machines. You can override this default if you want to install the VDA on an existing machine.

Description

Decide if you want to install Citrix Receiver for Windows (CitrixReceiver.exe).

You can disable this default action.

Decide how you want ports opened.

By default, the following ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. You can disable this default action and open the ports manually if you use a third-party firewall or no firewall, or if you just prefer to do it yourself.

- Controller: TCP 80, 1494, 2598, 8008
  - For communication between user devices and virtual desktops, configure inbound TCP on ports 1494 and 2598 as port exceptions. For security, Citrix recommends that you do not use these registered ports for anything other than the ICA protocol and the Common Gateway Protocol.
  - For communication between Controllers and virtual desktops, configure inbound port 80 as a port exception.
- Windows Remote Assistance: TCP 3389
  Windows opens this port automatically if the feature is enabled, even if you choose to open the ports manually.
- Real-Time Audio Transport: UDP 16500-16509

Tip: For complete port information, see CTX101810.

Decide how you will specify the locations of installed Controllers.

- Manually, by entering the Fully Qualified Domain Name (FQDN) of the Controller. Although you can specify a Controller that is not currently in the domain, a VDA can connect only to a Controller in the domain. Also, you can test the connection only for Controllers in the domain.
- Using Active Directory, if the Controller is in the domain.
- Allowing Machine Creation Services to specify the Controller.
- Later, by rerunning the installer, using Citrix policies, setting registry values, or using Active Directory OUs.

Citrix Group Policy settings that specify Controller locations will override settings provided during installation.

After you initially specify the Controller location, you can use the auto-update feature to update VDAs when additional Controllers are installed.

Decide if you want to use the following features:

- Optimize performance: When this feature is enabled, the optimization tool is used for VDAs running in a VM on a hypervisor. VM optimization includes disabling offline files, disabling background defragmentation, and reducing event log size. For more information, see CTX125874. Do not enable this option if you will be using Remote PC Access. Default = enabled.
- Windows Remote Assistance: When this feature is enabled, Windows Remote Assistance is used with the user shadowing feature of Director, and Windows automatically opens TCP port 3389 in the firewall, even if you choose to open firewall ports manually. Default = enabled.
- Real-Time Audio Transport for audio: When this feature is enabled, UDP is used for audio packets, which can improve audio performance. Default = enabled.
- Personal vDisk: (Available only when installing a VDA for Windows Desktop OS on a VM.) When this feature is enabled, Personal vDisks can be used with a master image. For more information, see Personal vDisks. Default = disabled.

Description

Good to know:

- The Print Spooler Service is enabled by default on the Windows server. If you disable this service, you cannot successfully install a VDA for Windows Server OS. Therefore, ensure that this service is enabled before installing a VDA.
- The installer automatically detects your operating system and allows you to install only the VDA type supported on that system: VDA for Windows Server OS or VDA for Windows Desktop OS.
- Profile management is installed during VDA installation.
- When you install the VDA, a new local user group called Direct Access Users is automatically created. On a VDA for Windows Desktop OS, this group applies only to RDP connections; on a VDA for Windows Server OS, this group applies to ICA and RDP connections.
- When you install a VDA for Windows Server OS, Remote Desktop Services role services are automatically installed and enabled (if they are not already installed and enabled).
- For Remote PC Access configurations, install the VDA for Windows Desktop OS on each physical office PC that users will access remotely.
- As an alternative to using the full-product ISO to install VDAs, you can use a standalone VDA installation package. For details, see Install VDAs using the standalone package.

Virtual Desktop Agents on Windows XP or Windows Vista

The latest Virtual Delivery Agents (VDAs) are not supported on Windows XP or Windows Vista systems. Additionally, some of the features in this release (and other recent releases) cannot be used on those operating systems. To use the full functionality in this release, Citrix recommends you replace Windows XP or Windows Vista systems with Windows 7, Windows 8 or Windows 10, then install a Virtual Delivery Agent from this release.

To accommodate cases when you must continue to accommodate machines running Windows XP or Windows Vista, you can install an earlier Virtual Desktop Agent version (5.6 FP1 with certain hotfixes). See CTX140941 for details.

Keep in mind that:

- You cannot install core components (Controller, Studio, Director, StoreFront, Citrix License Server) on a Windows XP or Windows Vista system.
- Remote PC Access is not supported on Windows Vista systems.
- Citrix support for Windows XP ended April 8, 2014 when Microsoft ended its extended support.
- Continuing to use older VDAs can affect feature availability and VDA registration with the Controller; see Mixed environment considerations.

Prepare the virtualization environment: VMware

Aug 31, 2016

Follow this guidance if you use VMware to provide virtual machines.

Install and configure your hypervisor

1. Install vCenter Server and the appropriate management tools. (No support is provided for vSphere vCenter Linked Mode operation.)
2. Create a VMware user account with the following permissions, at the DataCenter level, at a minimum. This account has permissions to create new VMs and is used to communicate with vCenter.

SDK	User Interface
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
System.Anonymous, System.Read, and System.View	Added automatically.
Task.Create	Tasks > Create task
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory

SDK	User Interface
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.Resource	Virtual machine > Configuration > Change resource
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Inventory.Register	Virtual machine > Inventory > Register
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.Provisioning.DiskRandomAccess	Virtual machine > Provisioning > Allow disk access
VirtualMachine.Provisioning.GetVmFiles	Virtual machine > Provisioning > Allow virtual machine download
VirtualMachine.Provisioning.PutVmFiles	Virtual machine > Provisioning > Allow virtual machine files upload
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template
VirtualMachine.Provisioning.MarkAsVM	Virtual machine > Provisioning > Mark as virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Create snapshot vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

SDK	User Interface
VirtualMachine.State.RemoveSnapshot	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Remove snapshot vSphere 5.5: Virtual machine > Snapshot management > Remove snapshot
VirtualMachine.State.RevertToSnapshot	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Revert to snapshot vSphere 5.5: Virtual machine > Snapshot management > Revert to snapshot

3. If you want the VMs you create to be tagged, add the following permissions for the user account:

SDK	User Interface
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

To ensure that you use a clean base image for creating new VMs, tag VMs created with Machine Creation Services to exclude them from the list of VMs available to use as base images.

Obtain and import a certificate

To protect vSphere communications, Citrix recommends that you use HTTPS rather than HTTP. HTTPS requires digital certificates. Citrix recommends you use a digital certificate issued from a certificate authority in accordance with your organization's security policy.

If you are unable to use a digital certificate issued from a certificate authority, and your organization's security policy permits it, you can use the VMware-installed self-signed certificate. Add the VMware vCenter certificate to each Controller. Follow this procedure:

1. Add the fully qualified domain name (FQDN) of the computer running vCenter Server to the hosts file on that server, located at %SystemRoot%/WINDOWS/system32/Drivers/etc/. This step is required only if the FQDN of the computer running vCenter Server is not already present in the domain name system.
2. Obtain the vCenter certificate using any of the following methods:
   - From the vCenter server:
     1. Copy the file rui.crt from the vCenter server to a location accessible on your Delivery Controllers.
     2. On the Controller, navigate to the location of the exported certificate and open the rui.crt file.
   - Download the certificate using a web browser. If you are using Internet Explorer, depending on your user account, you may need to right-click on Internet Explorer and choose Run as Administrator to download or install the certificate.
     1. Open your web browser and make a secure web connection to the vCenter server; for example https://server1.domain1.com
     2. Accept the security warnings.
     3. Click on the address bar where it shows the certificate error.

4. View the certificate and click on the Details tab.
5. Select Copy to file and export in .CER format, providing a name when prompted to do so.
6. Save the exported certificate.
7. Navigate to the location of the exported certificate and open the .CER file.

- Import directly from Internet Explorer running as an administrator:
  1. Open your web browser and make a secure web connection to the vCenter server; for example https://server1.domain1.com.
  2. Accept the security warnings.
  3. Click on the address bar where it shows the certificate error.
  4. View the certificate.
- Import the certificate into the certificate store on each of your Controllers:
  1. Click Install certificate, select Local Machine, and then click Next.
  2. Select Place all certificates in the following store, and then click Browse.
  3. If you are using Windows Server 2008 R2:
     1. Select the Show physical stores check box.
     2. Expand Trusted People.
     3. Select Local Computer.
     4. Click Next, then click Finish.

     If you are using Windows Server 2012 or Windows Server 2012 R2:
     1. Select Trusted People, then click OK.
     2. Click Next, then click Finish.

  Important: If you change the name of the vSphere server after installation, you must generate a new self-signed certificate on that server before importing the new certificate.

Create a master VM

Use a master VM to provide user desktops and applications.

1. Install a VDA on the master VM, selecting the option to optimize the desktop, which improves performance.
2. Take a snapshot of the master VM to use as a back-up. For more information, see Prepare a master image.

Create virtual desktops

If you are using Studio to create VMs, rather than selecting an existing machine catalog, specify the following information when setting up your hosting infrastructure to create virtual desktops.

1. Select the VMware vSphere host type.
2. Enter the address of the access point for the vCenter SDK (https://vmware.example.com/sdk).
3. Enter the credentials for the VMware user account you set up earlier that has permissions to create new VMs. Specify the username in the form domain/username.

Prepare the virtualization environment: Microsoft System Center Virtual Machine Manager

Sep 09, 2015

Follow this guidance if you use Hyper-V with Microsoft System Center Virtual Machine Manager (VMM) to provide virtual machines.

This release supports:

- VMM 2012 — Provides improved management capabilities, letting you manage the entire virtualized datacenter as well as virtual machines. This release now orchestrates cluster host patching as well as integrating with Windows Server Update Services, allowing you to define baselines of patches that each host needs.
- VMM 2012 SP1 — Provides performance improvements for Machine Creation Services (MCS) when using SMB 3.0 on file servers with clustered shared volumes and Storage Area Networks (SANs). These file shares provide low cost caching and reduced IO on the SAN storage improving the performance.
- VMM 2012 R2 — Enables at-scale management of major Windows Server 2012 R2 capabilities, including running VM snapshots, dynamic VHDX resize, and Storage Spaces.

This release supports only Generation 1 virtual machines with VMM 2012 R2. Generation 2 virtual machines are not supported for Machine Creation Services (MCS) and Provisioning Services deployments. When creating VMs with MCS or Provisioning Services, Generation 2 VMs do not appear in the selection list for a master VM; they have Secure Boot enabled by default, which prevents the VDA from functioning properly.

Upgrade VMM

- Upgrade from VMM 2012 to VMM 2012 SP1 or VMM 2012 R2
  For VMM and Hyper-V Hosts requirements, see http://technet.microsoft.com/en-us/library/gg610649.aspx. For VMM Console requirements, see http://technet.microsoft.com/en-us/library/gg610640.aspx.

  A mixed Hyper-V cluster is not supported. An example of a mixed cluster is one in which half the cluster is running Hyper-V 2008 and the other is running Hyper-V 2012.

- Upgrade from VMM 2008 R2 to VMM 2012 SP1
  If you are upgrading from XenDesktop 5.6 on VMM 2008 R2, follow this sequence to avoid XenDesktop downtime.
  1. Upgrade VMM to 2012 (now running XenDesktop 5.6 and VMM 2012)
  2. Upgrade XenDesktop to the latest version (now running the latest XenDesktop and VMM 2012)
  3. Upgrade VMM from 2012 to 2012 SP1 (now running the latest XenDesktop and VMM 2012 SP1)
- Upgrade from VMM 2012 SP1 to VMM 2012 R2
  If you are starting from XenDesktop or XenApp 7.x on VMM 2012 SP1, follow this sequence to avoid XenDesktop downtime.
  1. Upgrade XenDesktop or XenApp to the latest version (now running the latest XenDesktop or XenApp, and VMM 2012 SP1)
  2. Upgrade VMM 2012 SP1 to 2012 R2 (now running the latest XenDesktop or XenApp, and VMM 2012 R2)

Installation and configuration summary

1. Install and configure a hypervisor.
   1. Install Microsoft Hyper-V server and VMM on your servers. All Delivery Controllers must be in the same forest as the

VMM servers.

2. Install the System Center Virtual Machine Manager console on all Controllers.
3. Verify the following account information:
   - The account you use to specify hosts in Studio is a VMM administrator or VMM delegated administrator for the relevant Hyper-V machines. If this account only has the delegated administrator role in VMM, the storage data is not listed in Studio during the host creation process.
   - The user account used for Studio integration must also be a member of the administrators local security group on each Hyper-V server to support VM life cycle management (such as VM creation, update, and deletion).

   Note: Installing Controller on a server running Hyper-V is not supported.
2. Create a master VM.
   1. Install a Virtual Delivery Agent on the master VM, and select the option to optimize the desktop. This improves performance.
   2. Take a snapshot of the master VM to use as a backup.

   For more information, see Prepare a master image.

3. Create virtual desktops. If you are using MCS to create VMs, when creating a Site or a connection,
   1. Select the Microsoft virtualization host type.
   2. Enter the address as the fully qualified domain name of the host server.
   3. Enter the credentials for the administrator account you set up earlier that has permissions to create new VMs.
   4. In the Host Details dialog box, select the cluster or standalone host to use when creating new VMs.
      Important: Browse for and select a cluster or standalone host even if you are using a single Hyper-V host deployment.

MCS on SMB 3 file shares

For Machine Catalogs created with MCS on SMB 3 file shares for VM storage, make sure that credentials meet the following requirements so that calls from the Controller's Hypervisor Communications Library (HCL) connect successfully to SMB storage:

- VMM user credentials must include full read write access to the SMB storage.
- Storage virtual disk operations during VM life cycle events are performed through the Hyper-V server using the VMM user credentials.

When you use SMB as storage, enable the Authentication Credential Security Support Provider (CredSSP) from the Controller to individual Hyper-V machines when using VMM 2012 SP1 with Hyper-V on Windows Server 2012. For more information, see CTX137465.

Using a standard PowerShell V3 remote session, the HCL uses CredSSP to open a connection to the to Hyper-V machine. This feature passes Kerberos-encrypted user credentials to the Hyper-V machine, and the PowerShell commands in the session on the remote Hyper-V machine run with the credentials provided (in this case, those of the VMM user), so that communication commands to storage work correctly.

The following tasks use PowerShell scripts that originate in the HCL and are then sent to the Hyper-V machine to act on the SMB 3.0 storage.

- **Consolidate Master Image** - A master image creates a new MCS provisioning scheme (machine catalog). It clones and flattens the master VM ready for creating new VMs from the new disk created (and removes dependency on the original master VM).
  ConvertVirtualHardDisk on the root\virtualization\v2 namespace

  Example:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
```

```
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
```

- **Create difference disk** - Creates a difference disk from the master image generated by consolidating the master image. The difference disk is then attached to a new VM.
  CreateVirtualHardDisk on the root\virtualization\v2 namespace

  Example:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
```

- **Upload identity disks** - The HCL cannot directly upload the identity disk to SMB storage. Therefore, the Hyper-V machine must upload and copy the identity disk to the storage. Because the Hyper-V machine cannot read the disk from the Controller, the HCL must first copy the identity disk through the Hyper-V machine as follows.
  1. The HCL uploads the Identity to the Hyper-V machine through the administrator share.
  2. The Hyper-V machine copies the disk to the SMB storage through a PowerShell script running in the PowerShell remote session. A folder is created on the Hyper-V machine and the permissions on that folder are locked for the VMM user only (through the remote PowerShell connection).
  3. The HCL deletes the file from the administrator share.
  4. When the HCL completes the identity disk upload to the Hyper-V machine, the remote PowerShell session copies the identity disks to SMB storage and then deletes it from the Hyper-V machine.
     The identity disk folder is recreated if it is deleted so that it is available for reuse.

- **Download identity disks** - As with uploads, the identity disks pass though the Hyper-V machine to the HCL. The following process creates a folder that only has VMM user permissions on the Hyper-V server if it does not exist.
  1. The HyperV machine copies the disk from the SMB storage to local Hyper-V storage through a PowerShell script running in the PowerShell V3 remote session.
  2. HCL reads the disk from the Hyper-V machine's administrator share into memory.
  3. HCL deletes the file from the administrator share.
- **Personal vDisk creation** - If the administrator creates the VM in a Personal vDisk machine catalog, you must create an empty disk (PvD).
  The call to create an empty disk does not require direct access to the storage. If you have PvD disks that reside on different storage than the main or operating system disk, then the use remote PowerShell to create the PvD in a directory folder that has the same name of the VM from which it was created. For CSV or LocalStorage, do not use remote PowerShell. Creating the directory before creating an empty disk avoids VMM command failure.

  From the Hyper-V machine, perform a mkdir on the storage.

Prepare for using Microsoft System Center Configuration Manager

Sep 09, 2015

Sites that use System Center Configuration Manager (Configuration Manager) 2012 to manage access to applications and desktops on physical devices can extend that use to XenApp or XenDesktop through these integration options.

- **Citrix Connector 7.5 for Configuration Manager 2012 –** Citrix Connector provides a bridge between Configuration Manager and XenApp or XenDesktop. The Connector enables you to unify day-to-day operations across the physical environments you manage with Configuration Manager and the virtual environments you manage with XenApp or XenDesktop. For information about the Connector, see Citrix Connector 7.5 for System Center Configuration Manager 2012 .
- **Configuration Manager Wake Proxy feature –** Whether or not your environment includes Citrix Connector, the Remote PC Access Wake on LAN feature requires Configuration Manager. For more information, see Configuration Manager and Remote PC Access Wake on LAN.
- **XenApp and XenDesktop properties –** XenApp and XenDesktop properties enable you to identify Citrix virtual desktops for management through Configuration Manager. These properties are automatically used by the Citrix Connector but can also be manually configured, as described in the following section.

Properties

Properties are available to Microsoft System Center Configuration Manager 2012 and 2012 R2 to manage virtual desktops.

Boolean properties displayed in Configuration Manager 2012 may appear as 1 or 0, not true or false.

The properties are available for the Citrix_virtualDesktopInfo class in the Root\Citrix\DesktopInformation namespace. Property names come from the Windows Management Instrumentation (WMI) provider.

Property	Description
AssignmentType	Sets the value of IsAssigned. Valid values are: • ClientIP • ClientName • None • User – Sets IsAssigned to True
BrokerSiteName	Site; returns the same value as HostIdentifier.
DesktopCatalogName	Machine Catalog associated with the desktop.
DesktopGroupName	Delivery Group associated with the desktop.
HostIdentifier	Site; returns the same value as BrokerSiteName.
IsAssigned	True to assign the desktop to a user, set to False for a random desktop.

Property	Description
IsMasterImage	Allows decisions about the environment. For example, you may want to install applications on the Master Image and not on the provisioned machines, especially if those machines are in a clean state on boot machines. Valid values are: • True on a VM that is used as a master image (this value is set during installation based on a selection). • Cleared on a VM that is provisioned from that image.
IsVirtualMachine	True for a virtual machine, false for a physical machine.
OSChangesPersist	False if the desktop operating system image is reset to a clean state every time it is restarted; otherwise, true.
PersistentDataLocation	The location where Configuration Manager stores persistent data. This is not accessible to users.
PersonalvDiskDriveLetter	For a desktop with a Personal vDisk, the drive letter you assign to the Personal vDisk.
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	Determined when the desktop registers with the Controller; they are null for a desktop that has not fully registered.

To collect the properties, run a hardware inventory in Configuration Manager. To view the properties, use the Configuration Manager Resource Explorer. In these instances, the names may include spaces or vary slightly from the property names. For example, **BrokerSiteName** may appear as Broker Site Name. For information about the following tasks, see Citrix WMI Properties and System Center Configuration Manager 2012:

- Configure Configuration Manager to collect Citrix WMI properties from the Citrix VDA
- Create query-based device collections using Citrix WMI properties
- Create global conditions based on Citrix WMI properties
- Use global conditions to define application deployment type requirements

You can also use Microsoft properties in the Microsoft class CCM_DesktopMachine in the Root\ccm_vdi namespace. For more information, see the Microsoft documentation.

Configuration Manager and Remote PC Access Wake on LAN

For information about planning for and delivering Remote PC Access, see Remote PC Access and Provide users with Remote PC Access.

To configure the Remote PC Access Wake on LAN feature, complete the following before installing a VDA on the office PCs and using Studio to create or update the Remote PC Access deployment:

- Configure Configuration Manager 2012 within the organization, and then deploy the Configuration Manager client to all Remote PC Access machines, allowing time for the scheduled SCCM inventory cycle to run (or forcing one manually, if

required). The access credentials you specify in Studio to configure the connection to Configuration Manager must include collections in the scope and the Remote Tools Operator role.

- For Intel Active Management Technology (AMT) support:
  - The minimum supported version on the PC must be AMT 3.2.1.
  - Provision the PC for AMT use with certificates and associated provisioning processes.
- For Configuration Manager Wake Proxy and/or magic packet support:
  - Configure Wake on LAN in each PC's BIOS settings.
  - For Configuration Manager Wake Proxy support, enable the option in Configuration Manager. For each subnet in the organization that contains PCs that will use the Remote PC Access Wake on LAN feature, ensure that three or more machines can serve as sentinel machines.
  - For magic packet support, configure network routers and firewalls to allow magic packets to be sent, using either a subnet-directed broadcast or unicast.

After you install the VDA on office PCs, enable or disable power management when you create the Remote PC Access deployment in Studio.

- If you enable power management, specify connection details: the Configuration Manager address and access credentials, plus a name.
- If you do not enable power management, you can add a power management (Configuration Manager) connection later and then edit a Remote PC Access machine catalog to enable power management and specify the new power management connection.

You can edit a power management connection to configure the use of the Configuration Manager Wake Proxy and magic packets, as well as change the packet transmission method.

Install using the graphical interface

Oct 16, 2015

Before beginning any installation, review and complete the tasks in Prepare to install.

Launch the installer graphical interface:

1. Download the product package and unzip it. Optionally, burn a DVD of the ISO file.
2. Log on to the server where you are installing the components, using a local administrator account.
3. Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the AutoSelect application or the mounted drive.
4. Select the component you want to install:
   - If you're just getting started, select Delivery Controller. From there, you can install the Delivery Controller and optionally, Studio, Director, License Server, and StoreFront on the same server.
   - If you've already installed some components and want to extend your deployment, click the component you want to install from the right column. This column offers core components and the Universal Print Server, which you can install on your print server.
   - To install a Virtual Delivery Agent (VDA), click the available VDA entry - the installer knows which one is right for the operating system where you're running the installer.

Later, if you want to customize a VDA that you've already installed:

1. From the Windows feature for removing or changing programs, select Citrix Virtual Delivery Agent <version-number>, then right-click and select Change.
2. Select Customize Virtual Delivery Agent Settings. When the installer launches, you can change the Controller addresses, TCP/IP port to register with the Controller (default = 80), or whether to automatically open Windows Firewall port exceptions.

You can also use the graphical interface to upgrade components; see Upgrade a deployment.

As an alternative to using the full-product ISO to install VDAs, you can use a standalone VDA installation package. For details, see Install VDAs using the standalone package.

In XenApp and XenDesktop 7.6 FP3, the UPS package contains updated versions of the standalone UPS client and server components. For installation instructions, see the Install Citrix Universal Print Server (UPS) section in Provision printers.

Install using the command line

Aug 12, 2016

Use the command line interface to:

- Install one or more core components: Delivery Controller, Citrix Studio, Citrix Director, License Server, and StoreFront.
- Install a Virtual Delivery Agent (VDA) on a master image or on a virtual or physical machine.
  You can also customize scripts provided on the media, then use them to install and remove VDAs in Active Directory.
- Customize a previously-installed VDA.
- Install a Universal Print Server, which provisions network session printers. The Controller already has the Universal Print Server functionality; you need only install the Universal Print Server on the print servers in your environment.

You can also:

- Remove components from this version that you previously installed, using the /remove or /removeall options. For details, see Remove components.
- Upgrade components; for details, see Upgrade a deployment.

To see command execution progress and return values, you must be the original administrator or use 'Run as administrator.' For more information, see the Microsoft command documentation.

Important: Before beginning an installation, read and complete the tasks in Prepare to install.

Install core components using the command line

From the \x64\XenDesktop Setup directory on the media, run the XenDesktopServerSetup.exe command. The following table describes command options.
Note: To install XenApp, include the /xenapp option on the command line. To install XenDesktop, do not include the /xenapp option.

Option	Description
/help or /h	Displays command help.
/quiet or /passive	No user interface appears during the installation. The only evidence of the installation process is in Windows Task Manager. If this option is omitted, the graphical interface launches.
/logpath path	Log file location. The specified folder must already exist; the installer does not create it. Default = "%TEMP%\Citrix\XenDesktop Installer"
/noreboot	Prevents a restart after installation. (For most core components, a restart is not enabled by default.)
/remove	Removes the core components specified with the /components option.
/removeall	Removes all installed core components.
/xenapp	Installs XenApp. If this option is omitted, XenDesktop is installed.
/configure_firewall	Opens all ports in the Windows firewall needed by components being installed, if the Windows Firewall Service is running, even if the firewall is not enabled. If you are using a third-party firewall or no firewall, you must manually open the ports.
/components component [,component] ...	(Required.) Comma-separated list of components to install or remove. Valid values are: • CONTROLLER - Controller • DESKTOPSTUDIO - Studio • DESKTOPDIRECTOR - Director • LICENSESERVER - Citrix Licensing • STOREFRONT - StoreFront If this option is omitted, all components are installed (or removed, if the /remove option is also specified).
/installdir directory	Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.
/tempdir directory	Directory that holds temporary files during installation. Default = c:\Windows\Temp.
/nosql	Prevents installation of Microsoft SQL Server Express on the server where you are installing the Controller. If this option is omitted, SQL Server Express will be installed.
/no_remote_assistance	(Valid only when installing Director.) Prevents the installation and enabling of the Windows Remote Assistance feature.

For example, the following command installs a XenDesktop Controller, Studio, Citrix Licensing, and SQL Server Express on the server. Ports required for component communications will be opened automatically.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components
controller,desktopstudio,licenseserver /configure_firewall
```

The following command installs a XenApp Controller, Studio, and SQL Server Express on the server. Ports required for component communication will be opened automatically.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components
controller,desktopstudio /configure_firewall
```

Install a VDA using the command line

When installing a VDA for use with Remote PC Access, specify only options that are valid on physical machines (not VMs or master images) and for VDAs for Windows Desktop OS.

From the XenDesktop Setup directory on the product media, run the XenDesktopVdaSetup.exe command. The following table describes command options. Unless otherwise noted, options apply to physical and virtual machines, and to VDAs for Windows Desktop OS and VDAs for Windows Server OS.

Option	Description
/h or /help	Displays command help.
/quiet or /passive	No user interface appears during the installation. The only evidence of the installation and configuration process is in Windows Task Manager. If this option is omitted, the graphical interface launches.
/logpath path	Log file location. The specified folder must already exist; the installer does not create it. Default = "%TEMP%CitrixXenDesktop Installer"
/noreboot	Prevents a restart after installation. The VDA will not be fully available for use until after a restart.
/remove	Removes the components specified with the /components option.
/removeall	Removes all installed VDA components.
/reconfig	Customizes previously-configured VDA settings when used with the /portnumber, /controllers, or /enable_hdx_ports options. If you specify this option without also specifying the /quiet option, the graphical interface for customizing the VDA launches.
/portnumber port	(Valid only if the /reconfig option is specified.) Port number to enable for communications between the VDA and the Controller. The previously-configured port is disabled, unless it is port 80.
/components component[,component]	Comma-separated list of components to install or remove. Valid values are: • VDA - installs the VDA • PLUGINS - installs the Citrix Receiver for Windows (CitrixReceiver.exe) If this option is omitted, all components are installed.
/installdir directory	Existing empty directory where components will be installed. Default = c:Program FilesCitrix.
/tempdir directory	Directory to hold temporary files during installation. (This option is not available in the graphical interface.) Default = c:WindowsTemp.
/site_guid guid	Globally Unique Identifier of the site Active Directory Organizational Unit (OU). This associates a virtual desktop with a Site when you are using Active Directory for discovery (auto-update is the recommended and default discovery method). The site GUID is a site property displayed in Studio. Do not specify both the /site_guid and /controllers options.
/controllers "controller [controller] [...]"	Space-separated Fully Qualified Domain Names (FQDNs) of Controllers with which the VDA can communicate, enclosed in quotation marks. Do not specify both the /site_guid and /controllers options.
/xa_server_location url	URL of the server for Windows server applications.
/enable_remote_assistance	Enables Windows Remote Assistance for use with Director. If you specify this option, Windows opens TCP port 3389 in the firewall, even if you omit the /enable_hdx_ports option.
/enable_hdx_ports	Opens ports in the Windows firewall required by the Controller and features you specified (Windows Remote Assistance, real-time transport, and optimize), if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually.
/optimize	Enables optimization for VDAs running in a VM on a hypervisor. VM optimization includes disabling offline files, disabling background defragmentation, and reducing event log size. Do not specify this option for Remote PC Access. For more information about the optimization tool, see CTX125874.
/baseimage	(Valid only when installing a VDA for Windows Desktop OS on a VM.) Enables the use of Personal vDisks with a master image. For more information, see Personal vDisks.
/enable_hdx_3d_pro	Installs the VDA for HDX 3D Pro. For more information, see the HDX 3D Pro documentation.
/enable_real_time_transport	Enables or disables use of UDP for audio packets (Real-Time Audio Transport for audio). Enabling this feature can improve audio performance. Include the /enable_hdx_ports option if you want the UDP ports opened automatically if the Windows Firewall Service is detected.
/masterimage	(Valid only when installing a VDA on a VM.) Sets up the VDA as a master image.
/virtualmachine	(Valid only when installing a VDA on a VM.) Overrides detection by the installer of a physical machine, where BIOS information passed to VMs makes them appear as physical machines.

Option	Description
/nodesktopexperience	(Valid only when installing a VDA for Windows Server OS.) Prevents enabling of the Enhanced Desktop Experience feature. This feature is also controlled with the Enhanced Desktop Experience Citrix policy setting.
/nocitrixwddm	(Valid only on Windows 7 machines that do not include a WDDM driver.) Disables installation of the Citrix WDDM driver.
/servervdi	Installs a VDA for Windows Desktop OS on a supported Windows Server. Omit this option when installing a VDA for Windows Server OS on a Windows Server. Before using this option, see Server VDI. **Note:** Add the /masterimage option if you are installing the VDA on an image, and will use MCS to create server VMs from that image.
/installwithsecurebootenabled	Allows VDA installation when Secure Boot is enabled. If this option is omitted, a warning displays that Secure Boot must be disabled to successfully install a VDA.
/exclude "Personal vDisk","Machine Identity Service"	(Valid only when upgrading from an earlier 7.x VDA version on a physical machine.) Excludes Personal vDisk and Machine Identity Service from the upgrade. For advanced use of this option, see CTX140972.

For example, the following command installs a VDA for Windows Desktop OS and Citrix Receiver to the default location on a VM. This VDA will be used as a master image. The VDA will register initially with the Controller on the server named 'Contr-Main' in the domain 'mydomain,' and will use Personal vDisks, the optimization feature, and Windows Remote Assistance.

```
XenDesktop SetupXenDesktopVdaSetup.exe /quiet /components
vda,plugins /controllers "Contr-Main.mydomain.local" /enable_hdx_ports /optimize
/masterimage /baseimage /enable_remote_assistance
```

The following command installs a VDA for Windows Desktop OS and Citrix Receiver to the default location on an office PC that will be used with Remote PC Access. The machine will not be restarted after the VDA is installed; however, a restart is required before the VDA can be used. The VDA will register initially with the Controller on the server named 'Contr-East' in the domain 'mydomain,' and will use UDP for audio packets. HDX ports will be opened if the Windows Firewall service is detected.

```
XenDesktop SetupXenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-East.mydomain.local" /enable_hdx_ports /enable_real_time_transport /noreboc
```

As an alternative to using the full-product ISO to install VDAs, you can use a standalone VDA installation package. For details, see Install VDAs using the standalone package.

Customize a VDA using the command line

After you install a VDA, you can customize several settings. From the \x64\XenDesktop Setup directory on the product media, run the XenDesktopVdaSetup.exe command, using one or more of the following options, which are described above.

- /reconfigure - this option is required when customizing a VDA
- /h or /help
- /quiet
- /noreboot
- /controllers
- /portnumber port
- /enable_hdx_ports

Install the Universal Print Server using the command line

Notes:

- Deploying the Universal Print Server on 32-bit operating systems is not supported.
- User authentication during printing operations requires the Universal Print Server to be joined to the same domain as the Remote Desktop Services VDA.
- The UPClient component is part of the VDA installation; you do not need to manually install the client component.

To install the Universal Print Server using the command line:

- On a Windows 2008 R2 SP1, Windows Server 2012, or Windows Server 2012 R2 print server, run **UpsServer_x64.msi** from the \x64\Universal Print Server\ directory of the LTSR image.

If you install the Universal Print Server using the command line, we recommend that you add the command option, /ENABLE_CEIP set to 1, to opt in to the Citrix Customer Experience Improvement Program (CEIP).

For example:

Code COPY

```
<p>msiexec /i UpsServer.msi ENABLE_CEIP=1</p>
```

When you opt in, anonymous statistics and usage information is sent to Citrix to help improve the quality and performance of our products.

Create a Site

Sep 09, 2015

A Site is the name you give to a product deployment. It comprises the Delivery Controllers and the other core components, VDAs, virtual resource connections (if used), plus the machine catalogs and Delivery Groups you create and manage. A Site does not necessarily correspond to a geographical location, although it can. You create the Site after you install the components and before creating machine catalogs and Delivery Groups.

Prepare

The following table describes the tasks to complete and things to consider or be aware of before starting the Site creation wizard in Studio.

<table>
<tr><th></th><th>Description</th></tr>
<tr><td></td><td>Decide which type of Site you will create:
Application and desktop delivery Site - When you choose to create an application and desktop delivery Site, you can further choose to create a full deployment Site (recommended) or a empty Site. (Empty Sites are only partially configured, and are usually created by advanced users.)
Remote PC Access Site - Allows designated users to remotely access their office PCs through a secure connection. If you will use the Remote PC Access Wake on LAN feature, complete the tasks described in Configuration Manager and Remote PC Access Wake on LAN.
If you create an application and desktop delivery deployment now, you can add a Remote PC Access deployment later. Conversely, if you create a Remote PC Access deployment now, you can add a full deployment later.</td></tr>
<tr><td></td><td>Site creation includes creating the Site Configuration database. Make sure the SQL Server software is installed before you create a Site.

To create the database, you must be a local administrator and a domain user. You must also either have SQL Server permissions, or you can generate scripts to give to your database administrator to run.
Permissions – you need the following permissions when setting up the database; the permissions can be explicitly configured or acquired by Active Directory group membership:<table><tr><th>Operation</th><th>Purpose</th><th>Server role</th><th>Database role</th></tr><tr><td>Database creation</td><td>Create a suitable empty database</td><td>dbcreator</td><td></td></tr><tr><td>Schema creation</td><td>Create all service-specific schemas and add the first Controller to the Site</td><td>securityadmin *</td><td>db_owner</td></tr><tr><td>Add Controller</td><td>Add a Controller (other than the first) to the Site</td><td>securityadmin *</td><td>db_owner</td></tr><tr><td>Add Controller (mirror server)</td><td>Add a Controller login to the database server currently in the mirror role of a mirrored database</td><td>securityadmin *</td><td></td></tr></table></td></tr>
</table>

	Description	Purpose	Server role	Database role
	Schema update	Apply schema updates or hotfixes		db_owner

* While technically more restrictive, in practice, the securityadmin server role should be treated as equivalent to the sysadmin server role.

When using Studio to perform these operations, the user account must be a member of the sysadmin server role.

If your Studio user credentials do not include these permissions, you are prompted for SQL Server user credentials.

- Scripts - If your database server is locked down and you do not have the required SQL Server permissions, the Site creation wizard can generate two database scripts: one that sets up the database and the other to use in a mirroring environment. After you request script generation, you give the generated scripts to your database administrator (or someone with required SQL Server permissions) to run on the database server, and the mirrored database, if needed. After the script is executed and the database is successfully created, you can finish creating the Site.

Consider if you will use the 30-day free trial license that allows you to add license files later, or if you will use existing licenses. You can add or download license files from within the Site creation wizard.

Configure your virtualization resource (host) environment.

If you use XenServer:

- See the XenServer documentation.
- You must provide the credentials for a VM Power Admin or higher-level user.
- Citrix recommends using HTTPS to secure communications with XenServer. To use HTTPS, you must replace the default SSL certificate that was installed on XenServer with a certificate from a trusted authority; see CTX128656.
- You can configure high availability if it is enabled on the XenServer. Citrix recommends that you select all servers in the pool to allow communication with XenServer if the pool master fails. It can be selected from "Edit High Availablity" of added host.
- You can also select a GPU type and group, or passthrough, if the XenServer supports vGPU. The display indicates if the selection has dedicated GPU resources.

If you use VMware, see that product's documentation and Prepare the virtualization environment: VMware.

If you are using Hyper-V, see that product's documentation and Prepare the virtualization environment: Microsoft System Center Virtual Machine Manager.

Decide if you will use Machine Creation Services (MCS) or other tools to create VMs on the virtualization resources.

Decide if you will use shared or local storage. Shared storage is available through the network. If you use shared storage, you can enable the use of IntelliCache to reduce load on the storage device. For information, see Use IntelliCache for XenServer connections.

	Description
	Decide if you will use Personal vDisks and whether they will use shared or local storage. Personal vDisks can use the same or different storage as the VMs. If you installed product components in a cloud environment, you will need the API key and secret key values when configuring the first connection. You can export the key file containing those values from AWS or CloudPlatform, and then import them into the Site creation wizard. When you create a Site for a cloud deployment, you will also need the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials you configured in AWS.
	Decide if you will use App-V publishing, and configure those resources, if needed.

	Good to know:
	• When you create a Remote PC Access Site:
	  • A machine catalog named Remote PC Access Machines, and a Delivery Group named Remote PC Access Desktops are automatically created.
	  • You must specify users or user groups; there is no default action that automatically adds all users.
	  • You can enable the Wake on LAN feature (power management) and specify the Microsoft System Center Configuration Manager (ConfigMgr) address and credentials, plus a connection name.
	• The user who creates a Site becomes a Full Administrator; for more information, see Delegated Administration.
	• When an empty database is created, it has default attributes except:
	  • The collation sequence is set to Latin1_General_100_CI_AS_KS (where Latin1_General varies, depending on the country, for example Japanese_100_CI_AS_KS). If this collation setting is not specified during database creation, subsequent creation of the service schemas within the database will fail, and an error similar to "<service>: schema requires a case-insensitive database" appears. (When a database is created manually, any collation sequence can be used, provided it is case-sensitive, accent-sensitive, and kanatype-sensitive; the collation sequence name typically ends with _CI_AS_KS.)
	  • The recovery mode is set to Simple. For use as a mirrored database, change the recovery mode to Full.
	• When you create the Site Configuration Database, it also stores configuration changes recorded by the Configuration Logging Service, plus trend and performance data that is used by the Monitoring Service and displayed by Citrix Director. If you use those features and store more than seven days of data, Citrix recommends that you specify different locations for the Configuration Logging Database and the Monitoring Database (known as the secondary databases) after you create a Site.
	• When naming the Monitoring Database, or a Site Configuration Database that includes the Monitoring Database, using a name that includes spaces causes errors when the database is accessed. For more information, see to CTX200325.
	• At the end of the Site creation wizard, you are asked if you want to participate in the Citrix Customer Experience Improvement Program. When you join this program, anonymous statistics and usage information is sent to Citrix; see About the Citrix Customer Experience Improvement Program for more information.

Create

Start Studio, if it is not already open. After you choose to create a Site from the center pane, specify the following:

- The type of Site and the Site name.
- Database information. If you chose during Controller installation to have the default SQL Server Express database

installed, some information is already provided. If you use a database server that is installed on a different server, enter the database server and name:

Database type	What to enter	With this database configuration
Standalone or mirror	servername	The default instance is used and SQL Server uses the default port.
	servername\INSTANCENAME	A named instance is used and SQL Server uses the default port.
	servername,port-number	The default instance is used and SQL Server uses a custom port. (The comma is required.)
Other	cluster-name	A clustered database.
	availability-group-listener	An AlwaysOn database.

After you click Next and are alerted that the services could not connect to a database, indicate that you want Studio to create it. If you do not have permission to edit the database, use Generate database script. The scripts must be run before you can finish creating the Site.

- License Server address in the form name:[port], where name is a Fully Qualified Domain Name (FQDN), NetBIOS, or IP address; FQDN is the recommended format. If you omit the port number, the default is 27000. You cannot proceed until a successful connection is made to the license server.
- (Remote PC Access Sites only.) Power management information, including ConfigMgr connection information.
- Connection information to your virtualization resource and storage information. If you are not using a resource, or if you will use Studio to manage user desktops hosted on dedicated blade PCs, select the connection type None.
- App-V management and App-V publishing server information.
- (Remote PC Access Sites only.) User and machine accounts information.
  - User information. Click Add Users. Select users and user groups, and then click Add users.
  - Machine accounts information. Click Add machine accounts. Select machine accounts, and then click Add machine accounts. Click Add OUs. Select the domain and Organizational Units, and indicate if items in subfolders should be included. Click Add OUs.

Test a Site configuration

You can view an HTML report of the site test results. To run the tests:

1. From Studio, click the Studio (<site-name>) entry at the top of the left pane.
2. In the center pane, click Test site.

Install or remove Virtual Delivery Agents using scripts

Sep 29, 2015

The installation media contains sample scripts that install, upgrade, or remove Virtual Delivery Agents (VDAs) for groups of machines in Active Directory. You can also apply the scripts to individual machines, and use them to maintain master images used by Machine Creation Services and Provisioning Services.

Required access:

- The scripts need Everyone Read access to the network share where the VDA installation command is located. The installation command is XenDesktopVdaSetup.exe from the full product ISO, or VDAWorkstationSetup.exe or VDAServerSetup.exe from the standalone installer.
- Logging details are stored on each local machine. If you also want to log results centrally for review and analysis, the scripts need Everyone Read and Write access to the appropriate network share.

To check the results of running a script, examine the central log share. Captured logs include the script log, the installer log, and the MSI installation logs. Each installation or removal attempt is recorded in a time-stamped folder. The folder title indicates if the operation was successful with the prefix PASS or FAIL. You can use standard directory search tools to quickly find a failed installation or removal in the central log share, rather than searching locally on the target machines.

Important: Before beginning any installation, read and complete the tasks in Prepare to install.

1. Obtain the sample script InstallVDA.bat from \Support\AdDeploy\ on the installation media. Citrix recommends that you make a backup of the original script before customizing it.
2. Edit the script:
   - Specify the version of the VDA to install: `SET DESIREDVERSION`. For example, version 7 can be specified as 7.0; the full value can be found on the installation media in the ProductVersion.txt file (such as 7.0.0.3018); however, a complete match is not required.
   - Specify the network share location from which the installer will be invoked. Point to the root of the layout (the highest point of the tree): the appropriate version of the installer (32-bit or 64-bit) will be called automatically when the script runs. For example: `SET DEPLOYSHARE=\\fileserver1\share1`.
   - Optionally, specify a network share location for storing centralized logs. For example: `SET LOGSHARE=\\fileserver1\log1`).
   - Specify VDA configuration options as described in Install using the command line. The /quiet and /noreboot options are included by default in the script and are required: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT`.
3. Using Group Policy Startup Scripts, assign the script to the OU in Active Directory where your machines are located. This OU should contain only machines on which you want to install the VDA. When the machines in the OU are restarted, the script runs on all of them, installing a VDA on each machine that has a supported operating system.

1. Obtain the sample script UninstallVDA.bat from \Support\AdDeploy\ on the installation media. Citrix recommends that you make a backup of the original script before customizing it.
2. Edit the script.
   - Specify the version of the VDA to remove: `SET CHECK_VDA_VERSION`. For example, version 7 can be specified as 7.0; the full value can be found on the installation media in the ProductVersion.txt file (such as 7.0.0.3018); however, a complete match is not required.
   - Optionally, specify a network share location for storing centralized logs.

3. Using Group Policy Startup Scripts, assign the script to the OU in Active Directory where your machines are located. This OU should contain only machines from which you want to remove the VDA. When the machines in the OU are restarted, the script runs on all of them, removing a VDA from each machine.

The script generates internal log files that describe script execution progress. The script copies a Kickoff_VDA_Startup_Script log to the central log share within seconds of starting the deployment to the machine, so that you can verify that the overall process is working. If this log is not copied to the central log share as expected, you can troubleshoot further by inspecting the local machine: the script places two debugging log files in the %temp% folder on each machine, for early troubleshooting:

- Kickoff_VDA_Startup_Script_<DateTimeStamp>.log
- VDA_Install_ProcessLog_<DateTimeStamp>.log

Review the content of these logs to ensure that the script is:

- Running as expected.
- Properly detecting the target operating system.
- Correctly configured to point to the ROOT of the DEPLOYSHARE share (contains the file named AutoSelect.exe).
- Capable of authenticating to both the DEPLOYSHARE and LOG shares.

Install VDAs using the standalone package

Sep 16, 2016

As an alternative to using the full-product XenApp or XenDesktop ISO to install Virtual Delivery Agents (VDAs), you can use a standalone VDA installation package. The smaller package more easily accommodates deployments using Electronic Software Delivery (ESD) packages that are staged or copied locally, have physical machines, or have remote offices.

The standalone VDA package is intended primarily for deployments that use command-line (silent) installation - it supports the same command line parameters as the XenDesktopVdaSetup.exe command, which is used by the full-product installer. The package also offers a graphical interface that is very similar to the VDA installer on the full-product ISO.

There are two self-extracting standalone VDA packages: one for installation on supported server OS machines, and another for supported workstation (desktop) OS machines.

The supported operating systems for VDAs, plus other requirements before installation, are listed in System requirements for XenApp and XenDesktop 7.6. See Prepare to install for details about the information you provide and choices you make during VDA installation.

XenApp and XenDesktop 7.6 FP3. The VDA package automatically deploys prerequisites, if the machine does not already have them; this includes Visual C++ 2008, 2010 and 2013 Runtimes (32-bit and 64-bit) and .NET Framework 4.5.1.

This .NET requirement is skipped by the installer if Windows 10, which includes .NET 4.6, is installed on the desktop where you want to install the VDA.

XenApp and XenDesktop 7.6, 7.6 FP1 and 7.6 FP2. The VDA package automatically deploys prerequisites, if the machine does not already have them; this includes Microsoft Visual C++ 2005, 2008, and 2010 Runtimes (32-bit and 64-bit) and .NET Framework 4.5.1.

When installing on a supported server OS machine, the Remote Desktop Services (RDS) role services are installed and enabled before installing the VDA. Alternatively, you can install the prerequisites yourself before installing the VDA.

Exception: Verify that Windows Server 2008 R2 and Windows 7 machines have at least .NET 3.5.1 installed before you start the VDA installation.

About restarts

- A restart is required at the end of the VDA installation.
- To minimize the number of additional restarts needed during the installation sequence, ensure that .NET Framework 4.5.1 or 4.5.2 is installed before beginning the VDA installation. Also, for Windows Server OS machines, install and enable the RDS role services before installing the VDA. (Other prerequisites do not typically require machine restarts, so you can let the installer take care of those for you.)
- If you do not install prerequisites before beginning the VDA installation, and you specify the /noreboot option for a command line installation, you must manage the restarts. For example, when using automatic prerequisite deployment, the installer will suspend after installing RDS, waiting for a restart; be sure to run the command again after the restart, to continue with the VDA installation.

If you use the graphical interface or the command line interface option that runs the package, the files in the package are extracted to the Temp folder. More disk space is required on the machine when extracting to the Temp folder than when

using the full-product ISO. Files extracted to the Temp folder are not automatically deleted, but you can manually delete them (from C:\Windows\Temp\Ctx-*, where * is a random Globally Unique Identifier) after the installation completes.

Alternatively, use a third party utility that can extract cabinet archives from EXE files (such as 7-Zip) to extract the files to a directory of your choice, and then run the XenDesktopVdaSetup.exe command. In 7.6 FP3, you can use the /extract command with an absolute path. For more information, see How to use in the section below.

If your deployment uses Microsoft System Center Configuration Manager, a VDA installation might appear to fail with exit code 3, even though the VDA installed successfully. To avoid the misleading message, you can wrap your installation in a CMD script or change the success codes in your Configuration Manager package. For more information, see the forum discussion here.

Citrix Display Only Driver in XenApp and XenDesktop 7.6 FP3

The Citrix Display Only Driver (DOD) is the only installed and supported display driver on the XenDesktop Standard VDA on Windows 10.

The Citrix DOD has no GPU assist, even if a GPU or vGPU is present. All rendering is performed by the MS Basic Renderer in the software using the CPU. The Citrix DOD does not support Desktop Composition Redirection (DCR). The Citrix DOD is not installed or supported on XenApp.

Important: You must either have elevated administrative privileges before starting the installation, or use "Run as administrator."

1. Download the appropriate package to the machine where you will be installing the VDA. Citrix account credentials are required to access the download site.

Where are you installing the VDA?	Download this package
On a supported server OS machine	VDAServerSetup.exe
On a supported workstation (desktop) OS machine	VDAWorkstationSetup.exe

   For single user, single server OS deployments (for example, delivering Windows Server 2012 to one user for web development), use the VDAWorkstationSetup.exe package. For more information, see Server VDI.

2. Install the VDA using the graphical interface or the command line interface.
   Remember: You must either have elevated administrative privileges before starting the installation, or use **Run as administrator**.
   Using the graphical interface:

   Disable User Account Control (UAC), then right-click the downloaded package and choose **Run as administrator**. The installer launches and proceeds through the installation wizard. The restart at the end of the wizard is required before the VDA can be used in a site. (The wizard is the same as the one used in the full-product ISO to install a VDA; you will not encounter anything different.)

   Using the command line interface:

   You have two options:

- **Extract the files from the package and then run XenDesktopVdaSetup.exe.**

  XenApp and XenDesktop 7.6 FP3. To extract the files before installing, use /extract with the absolute path, for example:

  ```
  .\VDAWorkstationSetup.exe /extract %temp%\CitrixVDAInstallMedia
  ```

  Then, in a separate command, run XenDesktopVdaSetup.exe from the directory containing the extracted content. See Install using the command line and CTX140972 for parameter information.

  XenApp and XenDesktop 7.6, 7.6 FP1 and 7.6 FP2. Extract the files before installing, using a third party utility that can extract cabinet archives from EXE files (such as 7-Zip). Then, in a separate command, run XenDesktopVdaSetup.exe from the directory containing the extracted content. See Install using the command line and CTX140972 for parameter information.

- **Run the package.**
  Run the downloaded package as if it was the XenDesktopVdaSetup.exe command in everything except its name. See Install using the command line and CTX140972 for parameter information.

  For example, the most common installation command used for Remote PC Access installs a VDA on a physical office PC, without installing Citrix Receiver or Citrix Profile Manager. The machine will not automatically be restarted after the VDA is installed; however, a restart is required before the VDA can be used. The VDA will register initially with the Controller on the server named 'Contr-East'. Ports will be opened if the Windows Firewall Service is detected.

```
<p>VDAWorkstationSetup.exe /quiet /components vda /exclude &quot;Citrix User Profile Manager&quot; /controllers &quot
```

Note

Excluding Citrix Profile management from the installation (Using the /exclude "Citrix User Profile Manager" option) will affect monitoring and troubleshooting of VDAs with Citrix Director. On the User details and EndPoint pages, the Personalization panel and the Logon Duration panel will fail. On the Dashboard and Trends pages, the Average Logon Duration panel will display data only for machines that have Profile management installed.

Even if you are using a third party user profile management solution, it is recommended that you install and run the Citrix Profile management Service to avoid loss of monitoring and troubleshooting in Citrix Director (enabling the Citrix Profile management Service is not required).

Machine catalogs

Sep 09, 2015

Collections of physical or virtual machines are managed as a single entity called a session machine catalog. Many deployments create a master image or template on their host, and then use that in the machine catalog as a guide for Citrix tools (such as Machine Creation Services or Provisioning Services) to create VMs from the image/template. A catalog can also contain physical machines.

After you create a machine catalog, tests run automatically to ensure that it is configured correctly. When the tests complete, you can view a test report. You can also run the tests later on demand from Citrix Studio site-name in the Studio navigation pane.

After the tests complete, create a Delivery group.

Create a machine catalog

Apr 21, 2016

If you will use Citrix tools (Machine Creation Services or Provisioning Services) to create VMs for your deployment, prepare a master image or template on your host hypervisor. Then, create the machine catalog.

Make sure the host has sufficient processors, memory, and storage to accommodate the number of machines you will create.

The master image contains the operating system, non-virtualized applications, VDA, and other software. VMs are created in a machine catalog, based on a master image you created earlier and specify when you create the catalog.

Good to know:

- Master image is also known as clone image, golden image, or base image.
- Cloud deployments use templates rather than master images. See the template guidance
  - in Amazon Web Services, see Deploy XenApp and XenDesktop 7.5 and 7.6 with Amazon VPC
  - in Citrix CloudPlatform, see XenApp and XenDesktop concepts and deployment on CloudPlatform.

When using Provisioning Services, you can use a master image or a physical computer as the master target device.

- Remote PC Access machine catalogs do not use master images.
- Microsoft KMS activation considerations when using Machine Creation Services:
  - If your deployment includes 7.x VDAs with a XenServer 6.1 or 6.2, vSphere, or Microsoft System Center Virtual Machine Manager host, you do not need to manually re-arm Microsoft Windows or Microsoft Office.
  - If your deployment includes a 5.x VDA with a XenServer 6.0.2 host, see CTX128580.

Important: If you are using Provisioning Services or Machine Creation Services, do not run Sysprep on master images.

1. Using your hypervisor's management tool, create a new master image and then install the operating system, plus all service packs and updates.
   The number of vCPUs and amount of memory are not critical at this point because you can change those values when you create the machine catalog. However, be sure to configure the amount of hard disk space required for desktops and applications, because that value cannot be changed later or in the catalog.
2. Make sure that the hard disk is attached at device location 0. Most standard master image templates configure this location by default, but some custom templates may not.
3. Install and configure the following software on the master image:
   - Integration tools for your hypervisor (such as XenServer Tools, Hyper-V Integration Services, or VMware tools). If you omit this step, your applications and desktops might not function correctly.
   - A VDA for Windows Server OS or VDA for Windows Desktop OS (Citrix recommends installing the latest version to allow access to the newest features. During installation, enable the optimization option, which improves performance by reconfiguring certain Windows features.
   - Third-party tools as needed, such as anti-virus software or electronic software distribution agents. Configure services such as Windows Update with settings that are appropriate for users and the machine type.
   - Third-party applications that you are not virtualizing. Citrix recommends virtualizing applications because it significantly reduces costs by eliminating the need to update the master image after adding or reconfiguring an application. In addition, fewer installed applications reduce the size of the master image hard disks, which saves storage costs.

- App-V clients with the recommended settings, if you plan to publish App-V applications.
- When using Machine Creation Services, and you will localize Microsoft Windows, install the locales and language packs. During provisioning, when a snapshot is created, the provisioned VMs use the installed locales and language packs.

4. When using Provisioning Services, create a VHD file for the vDisk from your master target device before you join the master target device to a domain.
5. Join the master image to the domain where desktops and applications will be members, and make sure that the master image is available on the host where the machines will be created.
6. Citrix recommends that you create and name a snapshot of your master image so that it can be identified later. If you specify a master image rather than a snapshot when creating a machine catalog, Studio creates a snapshot, but you cannot name it.

Prepare a master image for GPU-capable machines on XenServer - When using XenServer for your hosting infrastructure, GPU-capable machines require a dedicated master image. Those VMs require video card drivers that support GPUs and must be configured to allow the VM to operate with software that uses the GPU for operations.

1. In XenCenter, create a VM with standard VGA, networks, and vCPU.
2. Update the VM configuration to enable GPU use (either Passthough or vGPU).
3. Install a supported operating system and enable RDP.
4. Install XenServer Tools and NVIDIA drivers.
5. Turn off the Virtual Network Computing (VNC) Admin Console to optimize performance, and then restart the VM.
6. You are prompted to use RDP. Using RDP, install the VDA and then restart the VM.
7. Optionally, create a snapshot for the VM as a baseline template for other GPU master images.
8. Using RDP, install customer-specific applications that are configured in XenCenter and use GPU capabilities.

Before you start the machine catalog creation wizard, review the following procedure to learn about the choices you will make and information you will supply. When you start the wizard, some of the items may not appear or they may have different titles, based on your environment and the selections you make.

From Studio:

- If you have created a Site but haven't yet created a machine catalog, Studio will guide you to the correct starting place to create a machine catalog.
- If you have already created a machine catalog and want to create another, select Machine Catalogs in the Studio navigation pane, and then select Create Machine Catalog in the Actions pane.

The wizard walks you through the items described below.

- Operating system
  Each catalog contains machines of only one type:
  - Windows Server OS – A Windows Server OS catalog provides desktops and applications that can be shared by multiple users.
  - Windows Desktop OS – A Windows Desktop OS catalog provides desktops and applications that are assigned to individual users.
  - Remote PC Access – A Remote PC Access catalog provides users with remote access to their physical office desktop machines. Remote PC Access does not require a VPN to provide security.

  Amazon Web Services (AWS) supports only Server OS machine catalogs (and Server VDI, see Server VDI), not Desktop OS or Remote PC Access catalogs.

- Machine management

Indicate whether machines in the catalog will be power managed through Studio:

- Machines are power managed through Studio or provisioned through a cloud environment (for example, VMs or blade PCs). This option is available only if you have a hypervisor or cloud environment connection already configured. You probably configured a connection when you created the Site. If not, you can create a new connection later and then edit the machine catalog.
- Machines are not power managed through Studio (for example, physical machines).

Indicate which tool you will use to deploy machines:

- Machine Creation Services (MCS) – Uses a master image or template to create and manage virtual machines.
  - MCS is not available for physical machines.
  - Machine catalogs in cloud environments use MCS.
- Provisioning Services – Manages target devices as a device collection. A Provisioning Services vDisk imaged from a master target device delivers desktops and applications.
- Other – A tool that manages machines already in the data center. Citrix recommends you use Microsoft System Center Configuration Manager or another third-party application to ensure that the machines in the catalog are consistent.

- Desktop experience
  For machine catalogs containing Desktop OS machines that will be used to deliver desktops:
  - Specify whether users will connect to a new (random) desktop each time they log on, or if they will connect to the same (static) desktop each time.
  - If users connect to the same desktop, specify what will happen to any changes they make on the desktop. You can save changes to a separate Personal vDisk or the user's local VM disk, or you can discard changes. (If you choose to save changes to the separate Personal vDisk, you specify the drive letter and size later in the wizard.)
- Master image or machine template
  Select the master image (non-cloud) or machine template (cloud) you created earlier. Remember: If you are using Provisioning Services or Machine Creation Services, do not run Sysprep on master images.

- Security
  (Cloud environments) Select one or more security groups for the VMs; these are shown only if the availability zone supports security groups. Choose whether machines will use shared hardware or account-dedicated hardware.

- Virtual machines or Device collection or VMs and users
  Specify how many virtual machines to create. You can choose how many virtual CPUs and the amount of memory (in MB) each machine will have. Each VM will have a 32 GB hard disk; this value is set in the master image, it cannot be changed in the catalog.

  If you indicated previously that user changes to desktops should be saved on a separate Personal vDisk, specify its size in gigabytes and the drive letter.

  If you plan to use multiple Network Interface Cards (NICs), associate a virtual network with each card. For example, you can assign one card to access a specific secure network, and another card to access a more commonly-used network. You can also add or remove NICs from this wizard.

- Machine accounts
  (Remote PC Access catalogs) Specify the Active Directory machine accounts or Organizational Units (OUs) to add that correspond to users or user groups.

  You can choose a previously-configured power management connection or elect not to use power management. If you want to use power management but a suitable connection hasn't been configured yet, you can create that connection

later and then edit the machine catalog to update the power management settings.

- Computer accounts
  Each machine in the catalog must have a corresponding Active Directory computer account. Indicate whether to create new accounts or use existing accounts, and the location for those accounts.
  If you use existing accounts, make sure you have enough unused computer accounts for the machines that will be created.

  You can browse Active Directory to locate the existing accounts, or you can import a .csv file that lists the account names. The imported file content must use the format:

  ```
  [ADComputerAccount]
  ADcomputeraccountname.domain
  ...
  ```

  For catalogs containing physical machines or existing machines, select or import existing accounts and assign each machine to both an Active Directory computer account and to a user account.

  For machines created with Provisioning Services, computer accounts for target devices are managed differently; see the Provisioning Services documentation.

  Also specify the account naming scheme for the machines that are created – hash marks (#) in the scheme represent sequential numbers or letters that will be included with additional name text you provide.

- Name and description
  On the final page of the creation wizard, you specify the name and description of the machine catalog. This information appears in Studio.

Manage machine catalogs

Sep 16, 2015

For random machine catalogs, you can maintain users' desktops by applying global changes (such as Windows updates, anti-virus software updates, operating system upgrades, or configuration changes) to the master image. Then modify the machine catalog to use the updated master image so users receive the updated desktop the next time they log on. You can make significant changes for large numbers of users in one operation.

For static and Remote PC Access machine catalogs, you must manage updates to users' desktops outside of Studio, either on an individual basis or collectively using third-party software distribution tools. For machines created through Provisioning Services, updates to users' desktops are propagated through the vDisk.

Citrix recommends that you save copies or snapshots of master images before you make updates. The database keeps a historical record of the master images used with each machine catalog. Do not delete, move, or rename master images. You can revert a machine catalog to use the previous version of the master image if users encounter problems with updates you deployed to their desktops, thereby minimizing user downtime.

Before you start:

- Make sure the virtualization host has sufficient processors, memory, and storage to accommodate the additional machines.
- Make sure that you have enough unused Active Directory computer accounts. If using existing accounts, keep in mind that the number of machines you can add is limited by the number of accounts available.
- If you will use Studio to create Active Directory computer accounts for the additional machines, you must also have appropriate domain administrator permission.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a machine catalog and then select Add machines in the Actions pane.
3. Select the number of virtual machines to add.
4. If you indicate that new Active Directory accounts should be created (this step is required if there are insufficient existing accounts for the number of VMs you are adding):
   - Select the domain and location where the accounts will be created.
   - Specify an account naming scheme, using hash marks to indicate where sequential numbers or letters will appear (a name cannot begin with a number). For example, a naming scheme of PC-Sales-## (with 0-9 selected) results in computer accounts named PC-Sales-01, PC-Sales-02 , PC-Sales-03, etc.

   If you indicate that existing Active Directory accounts should be used:
   - Either browse to the accounts or click Import and specify a .csv file containing account names. Make sure that there are enough accounts for all the machines you're adding.
   - Studio manages these accounts, so either allow Studio to reset the passwords for all the accounts or specify the account password (which must be the same for all accounts).

The machines are created as a background process, and can be lengthy when creating a large number of machines. Machine creation continues even if you close Studio.

1. Select Machine Catalogs in the Studio navigation pane.

2. Select a catalog and then select Edit Machine Catalog in the Actions pane.
3. (Remote PC Access catalogs only) On the Power Management page, you can change a Remote PC Access catalog's power management settings and select a power management connection. On the Organizational Units page, add or remove OUs.
   On the Description page, change the machine catalog description.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a catalog and then select Rename Machine Catalog in the Actions pane.
3. Enter the new name.

Before deleting a machine catalog, ensure that:

- All users are logged off and that no disconnected sessions are running.
- Maintenance mode is turned on for all machines in the catalog, and then all machines are shut down.
- The catalog is not associated with a Delivery Group.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a catalog and then select Delete Machine Catalog in the Actions pane.
3. Indicate whether the machines in the catalog should be deleted. If you choose to delete the machines, indicate whether the associated computer accounts should be left as-is, disabled, or deleted in Active Directory.

After you delete a machine from a catalog, users no longer can access it. Before deleting a machine, ensure that:

- User data is backed up or no longer required.
- All users are logged off. Turning on maintenance mode will stop users from connecting to a machine.
- Desktops are not powered on or suspended.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a catalog and then select View Machines in the Actions pane.
3. Select one or more machines and then click Turn On Maintenance Mode in the Actions pane.
4. Select Delete in the Actions pane.
5. Choose whether to delete the machines being removed. If you choose to delete the machines, select what to do with the associated Active Directory computer accounts:

In machine catalog	In Active Directory
Leave	Do not change
Remove	Do not remove
Remove	Disable
Remove	Delete

To manage Active Directory accounts in a machine catalog, you can:

- Free unused machine accounts by removing Active Directory computer accounts from Desktop OS and Server OS machine catalogs. Those accounts can then be used for other machines.
- Add accounts so that when more machines are added to the catalog, the computer accounts are already in place

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a machine catalog and then select Manage AD accounts in the Actions pane.
3. Choose whether to add or delete computer accounts.
   - If you add accounts, you are prompted to specify what to do with the account passwords: either reset them all or enter a password that applies to all accounts. You might reset passwords if you do not know the current account passwords; you must have permission to perform a password reset. If you enter a password, the password will be changed on the accounts as they are imported.
   - If you delete an account, you are prompted to choose whether the account in Active Directory should be kept, disabled, or deleted.

Update a master image to apply changes to all the desktops and applications in a machine catalog that were created with that master image. Managing common aspects through a single master image lets you deploy system-wide changes such as Windows updates or configuration changes to a large number of machines quickly.

After preparing and testing a new/updated master image on the host (see Prepare a master image), modify the machine catalog to use it.

Note the following:

- Citrix recommends that you save copies or snapshots of master images before you make updates. The database keeps a historical record of the master images used with each machine catalog. You can revert a machine catalog to use the previous version of the master image if users encounter problems with updates you deployed to their desktops, thereby minimizing user downtime. Do not delete, move, or rename master images; otherwise, you will not be able to revert a machine catalog to use them.
  Although Studio can create a snapshot, Citrix recommends that you create a snapshot using the hypervisor management console, and then select that snapshot in Studio. This enables you to provide a meaningful name and description rather than an automatically generated name.

- For GPU master images, you can change the master image only through the XenServer XenCenter console.
- For machine catalogs that use Provisioning Services, you must publish a new vDisk to apply changes to the catalog. For details, see the Provisioning Services documentation.
- After updating the master image, you must restart the machines through Studio for the changes to take effect and be available to your users. This may occur automatically; for example, when a user logs off a desktop, or it may occur as part of a configured restart schedule. Alternatively, you can restart a machine from Studio.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a machine catalog and then select Update Machines in the Actions pane.
3. On the Master Image page, select the host and the new/updated master image.
4. On the Rollout Strategy page, specify when the new or updated master image is applied to users' machines: on the next shutdown or immediately.
   - If you choose to update the image on the next shutdown, you can notify users of the update.

- If you choose to update the image immediately, you can specify whether to restart all machines at the same time or at specified intervals. You can send a notification message to users 1, 5, or 15 minutes before they are logged off and the machine restarted.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select the machine catalog and then select Rollback machine update in the Actions pane.
3. Specify how to apply the reverted master image to user desktops, as described above.

The rollback strategy is applied only to desktops that need to be reverted. For desktops that have not been updated with the new/updated master image that prompted the rollback (for example, desktops with users who have not logged off), users do not receive messages and are not forced to log off.

Upgrade the machine catalog after you upgrade the VDAs on the machines to a newer version. Citrix recommends upgrading all VDAs to the latest version so they can all access the newest features.

Note: If you have Windows XP or Windows Vista machines, they must use an earlier VDA version, and will not be able to use the latest product features. If you cannot upgrade those machines to a currently supported Windows operating system, Citrix recommends you keep them in a separate machine catalog. For more information, see VDAs on machines running Windows XP or Windows Vista and Mixed VDA support.

Before you upgrade a machine catalog:

- If you're using Provisioning Services, upgrade the VDA version in the Provisioning Services console.
- Start the upgraded machines so that they register with the Controller. This lets Studio determine that the machines in the machine catalog need upgrading.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select the machine catalog. The Details tab in the lower pane displays version information.
3. Select Upgrade Catalog.
   - If Studio detects that the catalog needs upgrading, it displays a message. Follow the prompts.
   - If one or more machines cannot be upgraded, a message explains why. Citrix recommends you resolve machine issues before upgrading the machine catalog to ensure that all machines function properly.

Before you revert a machine catalog upgrade, if you used Provisioning Services to create the machine catalog, change the VDA version in the Provisioning Services console.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select the machine catalog. The Details tab in the lower pane displays version information.
3. Select Undo and then follow the prompts.

Delivery groups

Sep 09, 2015

A Delivery group is a collection of machines selected from one or more machine catalogs. The Delivery group specifies which users can use those machines, and the applications available to those users.

Begin by creating the Delivery group. Later, you can change the initial settings and configure additional ones.

To create a Delivery Group:

1. Select Delivery Groups in the Studio navigation pane.
2. Select Create Delivery Group in the Actions pane. The wizard walks you through the items described below.

Select a machine catalog and specify the number of machines you want to use from the catalog.

- At least one machine must remain unused in the selected machine catalog.
- A machine catalog can be specified in more than one Delivery group; however, a machine can be used in only one Delivery group.
- A Delivery group can use more than one machine catalog; however, those catalogs must contain the same machine types (Server OS, Desktop OS, or Remote PC Access). In other words, you cannot mix machine types in a Delivery group or in a machine catalog.
- Similarly, you cannot create a Delivery group containing Desktop OS machines from a machine catalog configured for static desktops and machines from a machine catalog configured for random desktops.
- Each machine in a Remote PC Access machine catalog is automatically associated with a Delivery group.

The type indicates what the Delivery group offers: only desktops, only applications, or both desktops and applications. Delivery groups with static Desktop OS machines cannot offer both desktops and applications.

Specify the users and user groups who can use the applications and/or desktops in the Delivery group.

There are two types of users: authenticated and unauthenticated (unauthenticated is also called anonymous). You can configure one or both types.

- **Authenticated** - The users and group members you specify by name must present credentials (such as smart card or user name and password) to StoreFront or Citrix Receiver to access applications and desktops.
- **Unauthenticated (anonymous)** - For Delivery Groups containing Server OS machines, you can select a check box that will allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. For example, when users access applications through kiosks, the application might require credentials, but the Citrix access portal and tools do not. An Anonymous Users Group is created when you install the VDA.
  - To grant access to unauthenticated users, each machine in the Delivery Group must have a VDA for Windows Server OS (minimum version 7.6) installed. When unauthenticated users are enabled, you must have an unauthenticated StoreFront store.
  - Unauthenticated user accounts are created on demand when a session is launched, and named AnonXYZ, in which XYZ is a unique three-digit value.

- Unauthenticated user sessions have a default idle timeout of 10 minutes, and are logged off automatically when the client disconnects. Reconnection, roaming between clients, and Workspace Control are not supported.

The following table describes your choices.

Enable access for	Add/assign users and user groups?	Enable the "Give access to unauthenticated users" check box?
Only authenticated users	Yes	No
Only unauthenticated users	No	Yes
Both authenticated and unauthenticated users	Yes	Yes

For Desktop groups containing Desktop OS machines, you can import user data (a list of users) after you create the Delivery group. See Import or export user lists.

A list displays the applications that were discovered on a machine created from the master image, a template in the machine catalog, or on the App-V management server. Choose one or more applications to add to the Delivery group.

You can also add (create) applications manually. You'll need to provide the path to the executable, working directory, optional command line arguments, and display names for administrators and users.

You can change an application's properties; see Change application properties for details.

You cannot create applications for Remote PC Access Delivery groups.

By default, applications you add are placed in a folder named Applications. Folders can make it easier to manage large numbers of applications. You can specify a different folder when you add the application; however, it's easier to manage folders later. See Manage application folders for details.

If you publish two applications with the same name to the same users, change the Application name (for user) property in Studio; otherwise, users will see duplicate names in Receiver.

Select or add StoreFront URLs that will be used by the Citrix Receiver that is installed on each machine in the Delivery group. You can also specify the StoreFront server address later by selecting Configuration > StoreFront in the navigation pane. When adding the StoreFront Server add '/Discovery' to the end of the URL.

Settings

Apr 27, 2015

The following documents describe how to configure and manage most of the settings you can specify and update for Delivery Groups:

- Applications
- Machines
- Remote PC Access
- Session
- Users

The information below describes settings that are not covered in those documents.

Before changing an application only or desktop and applications Delivery group to a desktop only Delivery group, delete all applications from the Delivery group.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery group, and then select Edit Delivery Group in the Actions pane.
3. On the Delivery Type page, select the delivery type you want to change the Deliver group to.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery group, and then select Edit Delivery Group in the Actions pane.
3. On the Basic Settings page, you can change the following:

Setting	Description
Description	The text that StoreFront uses and that users see.
Enabled check box	Whether or not the Delivery Group is enabled.
Desktops per user	(Desktop OS machines only) The maximum number of shared desktops that a user can have active at the same time. In assign-on-first-use deployments, this value specifies how many desktops users can assign to themselves.
Time zone	
Enable Secure ICA	Secures communications to and from machines in the Delivery Group using SecureICA, which encrypts the ICA protocol (default level is 128-bit; the level can be changed using the SDK). Citrix recommends using additional encryption methods such as SSL/TLS encryption when traversing public networks. Also, SecureICA does not check data integrity.

Upgrade a Delivery Group after you upgrade the VDAs on its machines.

Note: If you must continue using earlier VDA versions, newer product features may not be available. For more information, see Upgrade a deployment.

Before you start the Delivery Group upgrade:

- If you use Provisioning Services, upgrade the VDA version in the Provisioning Services console.
- Start the machines containing the new VDA so that they can register with the Controller. This process tells Studio what needs upgrading in the Delivery Group.

1. Select Delivery Groups in the Studio navigation pane.
2. Select the Delivery group and then select Upgrade Delivery Group in the Actions pane.

Before starting the upgrade process, Studio tells you which, if any, machines cannot be upgraded and why. You can then cancel the upgrade, resolve the machine issues, and then start the Delivery Group upgrade again.

After the Delivery Group upgrade completes, you can revert the machines to their previous states by selecting the Delivery Group and then selecting Undo in the Actions pane.

Machines

Jan 31, 2017

Unless otherwise noted, the following procedures are supported for all Delivery Group types: Server OS, Desktop OS, and Remote PC Access.

Note: This procedure is not supported for Remote PC Access machines.

1. Select Delivery Groups in the Studio navigation pane.
2. Select the Delivery Group and then select View Machines in the Actions pane.
3. Select the machine and select one of the following in the Actions pane (some options may not be available, depending on the machine state):
   - Force shut down — Forcibly powers off the machine and refreshes the list of machines.
   - Restart — Requests the operating system to shut down and then start the machine again. If the operating system cannot comply, the machine remains in its current state.
   - Suspend — Pauses the machine without shutting it down, and refreshes the list of machines.
   - Shut down — Requests the operating system to shut down.

If the machine does not shut down within 10 minutes, it is powered off. If Windows attempts to install updates during the shutdown, there is a risk that the machine will be powered off before the updates finish.

Note: Citrix recommends that you prevent Desktop OS machine users from selecting Shut Down within a session. See the Microsoft policy documentation for details.

Note: You can power manage only virtual Desktop OS machines, not physical ones (including Remote PC Access machines). Desktop OS machines with GPU capabilities cannot be suspended, so power off operations fail. For Server OS machines, see Create a restart schedule

Machines can be in one of the following states:

Delivery Group	State
Random	Randomly allocated and in use
	Unallocated and unconnected
Static (assigned)	Permanently allocated and in use
	Permanently allocated and unconnected (but ready)
	Unallocated and unconnected

During normal use, static Delivery Groups typically contain both permanently allocated and unallocated machines. Initially, all machines are unallocated (except for those manually allocated when the Delivery Group was created). As users connect, machines become permanently allocated. You can fully power manage the unallocated machines in those Delivery Groups,

but only partially manage the permanently allocated machines.

- **Pools and buffers** - For random Delivery Groups and unallocated machines in static Delivery Groups, a pool is a set of unallocated (or temporarily allocated) machines that are kept in a powered-on state, ready for users to connect; a user gets a machine immediately after log on. The pool size (the number of machines kept powered-on) is configurable by time of day. (For static Delivery Groups, use the SDK to configure the pool.)
  A buffer is an additional standby set of unallocated machines that are turned on when the number of machines in the pool falls below a threshold that is a percentage of the Delivery Group size. For large Delivery Groups, a significant number of machines might be turned on when the threshold is exceeded, so plan Delivery Group sizes carefully or use the SDK to adjust the default buffer size.

- **Power state timers** - You can use power state timers to suspend machines after users have disconnected for a specified amount of time. For example, machines will suspend automatically outside of office hours if users have been disconnected for at least ten minutes. Random machines or machines with Personal vDisks automatically shut down when users log off, unless you configure the ShutdownDesktopsAfterUse Delivery Group property in the SDK.
  You can configure timers for weekdays and weekends, and for peak and nonpeak intervals.

- **Partial power management of permanently allocated machines** - For permanently allocated machines, you can set power state timers, but not pools or buffers. The machines are turned on at the start of each peak period, and turned off at the start of each off-peak period; you do not have the fine control that you have with unallocated machines over the number of machines that become available to compensate for machines that are consumed.

To power manage virtual Desktop OS machines:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane.
3. On the Power Management page, select Weekdays in the Power manage machines dropdown. (By default, weekdays are Monday to Friday.)
4. For random Delivery Groups, in Machines to be powered on, select Edit and then specify the pool size during weekdays. Then, select the number of machines to power on.
5. In Peak hours, set the peak and off-peak hours for each day.
6. Set the power state timers for peak and non-peak hours during weekdays:
   - In During peak hours > When disconnected, specify the delay (in minutes) before suspending any disconnected machine in the Delivery Group, and select Suspend.
   - In During off-peak hours > When disconnected, specify the delay before turning off any logged-off machine in the Delivery Group, and select Shutdown. This timer is not available for Delivery Groups with random machines.
7. Select Weekend in the Power manage machines dropdown, and then configure the peak hours and power state timers for weekends.

Use the SDK to:

- Shut down, rather than suspend, machines in response to power state timers, or if you want the timers to be based on logoffs, rather than disconnections.
- Change the default weekday and weekend definitions.

Note: You can use a restart schedule for Server OS machines only. For Desktop OS machines, see Power manage machines.

To configure a restart schedule:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane,
3. On the Restart Schedule page:

- In the Restart machines drop-down, choose how often to restart the machines.
- In the Restart first group at fields, specify the hour and minute (in 24-hour format) when the first server will begin the restart process.
- In the Restart additional groups every drop-down, Indicate whether all servers should be restarted at once, or how much time should be allowed to restart every server in the Delivery Group.
  For example, assume a Delivery Group has five servers, a Restart first group at time of 13:00 (1:00 pm), and a Restart additional groups every selection of 1 hour. That duration (60 minutes) is divided by the number of machines (five), which yields a restart interval of 12 minutes. So, the restart times are 1:00 pm, 1:12 pm, 1:24 pm, 1:36 pm, and 1:48 pm. This gives all five machines the chance to complete their restart at the end of the specified interval (1 hour).

- Indicate whether you want to send a message to users at a specified interval before they are logged off. The notification will be sent relative to each server's calculated restart time, as described in the example.

You cannot perform an automated power-on or shutdown in Studio.

When you need to temporarily stop new connections to machines, you can turn on maintenance mode for one or all the machines in a Delivery Group. You might do this before applying patches or using management tools.

- When a Server OS machine is in maintenance mode, users can connect to existing sessions, but cannot start new sessions.
- When a Desktop OS machine (or a PC using Remote PC Access) is in maintenance mode, users cannot connect or reconnect. Current connections remain connected until they disconnect or log off.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group.
3. To turn on maintenance mode for all machines in the Delivery Group, select Turn On Maintenance Mode in the Actions pane.
   To turn on maintenance mode for one machine:
   1. Select View Machines in the Actions pane.
   2. Select a machine, and then select Turn On Maintenance Mode in the Actions pane.
4. To turn maintenance mode off for one or all machines in a Delivery Group, follow the previous instructions, but select Turn Off Maintenance Mode in the Actions pane.

Windows Remote Desktop Connection (RDC) settings also affect whether a Server OS machine is in maintenance mode. Maintenance mode is on when any of the following occur:

- Server maintenance mode is set to on, as described above.
- RDC is set to Don't allow connections to this computer.
- RDC is not set to Don't allow connections to this computer, and the Remote Host Configuration User Logon Mode setting is one of the following:
  - Allow reconnections, but prevent new logons
  - Allow reconnections, but prevent new logons until the server is restarted.

Note: You can reallocate only Desktop OS machines, not Server OS machines or machines created through Provisioning Services.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group.
3. To reallocate more than one machine:

1. Select Edit Delivery Group in the Actions pane.
2. On the Machine Allocation (User Assignment) page, select machines and specify the new users.

4. To reallocate one machine:
   1. Select View Machines in the Actions pane.
   2. Select a machine, and then select Change User in the Actions pane.
   3. Add or remove the user.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane.
3. On the User Settings page, set the desktops per user value.

Note: You can use tags only on Desktop OS machines.
You can use tags to refine a machine search or to limit machine access. You can add any number of tags of any length.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select View Machines in the Actions pane.
3. Select a machine.
4. To add tags, select Add Tag in the Actions menu and then enter one or more tags, separated by semicolons (;).
   To change or remove tags, select Edit Tags in the Actions menu and then make the necessary changes.

Note: You can load manage Server OS machines only.
Load Management measures the server load and determines which server to select under the current environment conditions. This selection is based on:

- **Server maintenance mode status** – a Server OS machine is considered for load balancing only when maintenance mode is off. (See Prevent users from connecting to a machine (maintenance mode) for details.)
- **Server load index** – determines how likely a server delivering Server OS machines is to receive connections. The index is a combination of load evaluators: the number of sessions and the settings for performance metrics such as CPU, disk, and memory use. You specify the load evaluators in load management policy settings.
  - You can monitor the load index in Director, Studio search, and the SDK.
  - In Studio, the Server Load Index column is hidden by default. To display it, select a machine, right-select a column heading and then choose Select Column. In the Machine category, select Load Index.
  - In the SDK, use the Get-BrokerMachine cmdlet.

  A server load index of 10000 indicates that the server is fully loaded. If no other servers are available, users might receive a message that the desktop or application is currently unavailable when they launch a session.

- **Concurrent logon tolerance policy setting** - the maximum number of concurrent requests to log on to the server. (This setting is equivalent to load throttling in XenApp versions earlier than 7.5.)

If all servers are at or higher than the concurrent logon tolerance setting, the next logon request is assigned to the server with the lowest pending logons. If more than one server meets this criteria, the server with the lowest load index is selected.

For more information, see the
— Policy settings reference
.

Removing a machine deletes it from a Delivery Group but does not delete it from the machine catalog that the Delivery Group uses. Therefore, the machines are available for assignment to other Delivery Groups.

Machines must be shut down before they can be removed. To temporarily stop users from connecting to a machine while you are removing it, put the machine into maintenance mode before shutting it down.

Keep in mind that machines may contain personal data, so use caution before allocating the machine to another user. You may want to reimage the machine.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group and the select View Machines in the Actions pane.
3. Make sure that the machine is shut down.
4. Select Remove from Delivery Group in the Actions pane.

Any changes you make to restrict access to machines in a Delivery Group supersede previous settings, regardless of the method you use. You can:

- Restrict access for administrators using Delegated Administration scopes. You can create and assign a scope that permits administrators to access all applications, and another scope that provides access to only certain applications. See the Delegated Administration documentation for details.
- Restrict access for users through SmartAccess policy expressions that filter user connections made through NetScaler Gateway.
  1. Select Delivery Groups in the Studio navigation pane.
  2. Select the Delivery Group and then select Edit Delivery Group in the Actions pane.
  3. On the Access policy page, select Connections through NetScaler Gateway.
  4. To choose a subset of those connections, select Connections meeting any of the following filters. Then define the NetScaler Gateway site, and add, edit, or remove the SmartAccess policy expressions for the allowed user access scenarios. For details, see the NetScaler Gateway documentation.
- Restrict access for users through exclusion filters on access policies that you set in the SDK. Access policies are applied to Delivery Groups to refine connections. For example, you can restrict machine access to a subset of users, and you can specify allowed user devices. Exclusion filters further refine access policies. For example, for security you can deny access to a subset of users or devices.
  By default, exclusion filters are disabled.

  For example, for a teaching lab on a subnet in the corporate network, to prevent access from that lab to a particular Delivery Group, regardless of who is using the machines in the lab, use the following command: Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -

  You can use the asterisk (*) wildcard to match all tags that start with the same policy expression. For example, if you add the tag VPDesktops_Direct to one machine and VPDesktops_Test to another, setting the tag in the Set-BrokerAccessPolicy script to VPDesktops_* applies the filter to both machines.

1. Select Delivery Groups in the Studio navigation pane.
2. Select the Delivery Group, select View Machines in the Action pane.
3. Select a machine and then select Update machines in the Actions pane.
   - To choose a different master image, select Master image. Then select a snapshot. Expanding a selected snapshot

displays associated master images.

- To apply changes and notify machine users, select Rollout notification to end-users. Then specify:
  - When to update the master image: now or on the next restart.
  - The restart distribution time: all machines at the same time or at time variations.
  - If and when users will be notified of the restart, plus the message they will receive.

Applications

Sep 30, 2014

To add an application to a Delivery Group:
1. Select Delivery Groups in the Studio navigation pane.
2. Select the Delivery Group.
3. Select Add Applications in the Actions pane.

A list displays the applications that were discovered on a machine created from the master image, a template in the machine catalog, or on the App-V management server. Choose one or more applications to add to the Delivery Group.

You can also add (create) applications manually. You'll need to provide the path to the executable, working directory, optional command line arguments, and display names for administrators and users.

You can change an application's properties; see below.

By default, applications you add are placed in a folder named Applications. For more information about application folders, see below.

To duplicate, disable, rename, edit tags, or delete an application:
1. Select Delivery Groups in the Studio navigation pane.
2. Select the Applications tab in the middle pane and then select the application.
3. Select the appropriate task in the Actions pane.

Good to know:
- When you duplicate an application, it is automatically renamed and placed adjacent to the original.
- Deleting an application removes it from the Delivery Group but not from the master image.
- To move an application to a different application folder, see below.

To change the properties of an application:
1. Select Delivery Groups in the Studio navigation pane.
2. Select the Applications tab in the middle pane and then select the application.
3. Select Properties in the Actions pane.

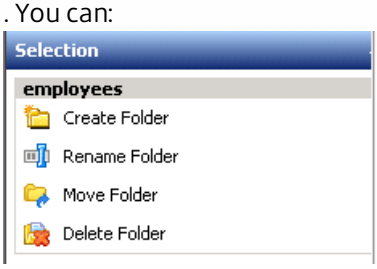
You can view and change the following:

Property to view or change	Select this page
Application name	Identification
Category in Receiver	Delivery
Command line arguments	Location

Property to view or change	Select this page
File extensions	File Type Association
File type association	File Type Association
Icon	Delivery
Keywords for StoreFront	Identification
Path to executable	Location
Shortcut on user's desktop	Delivery
Visibility	Limit Visibility
Working directory	Location

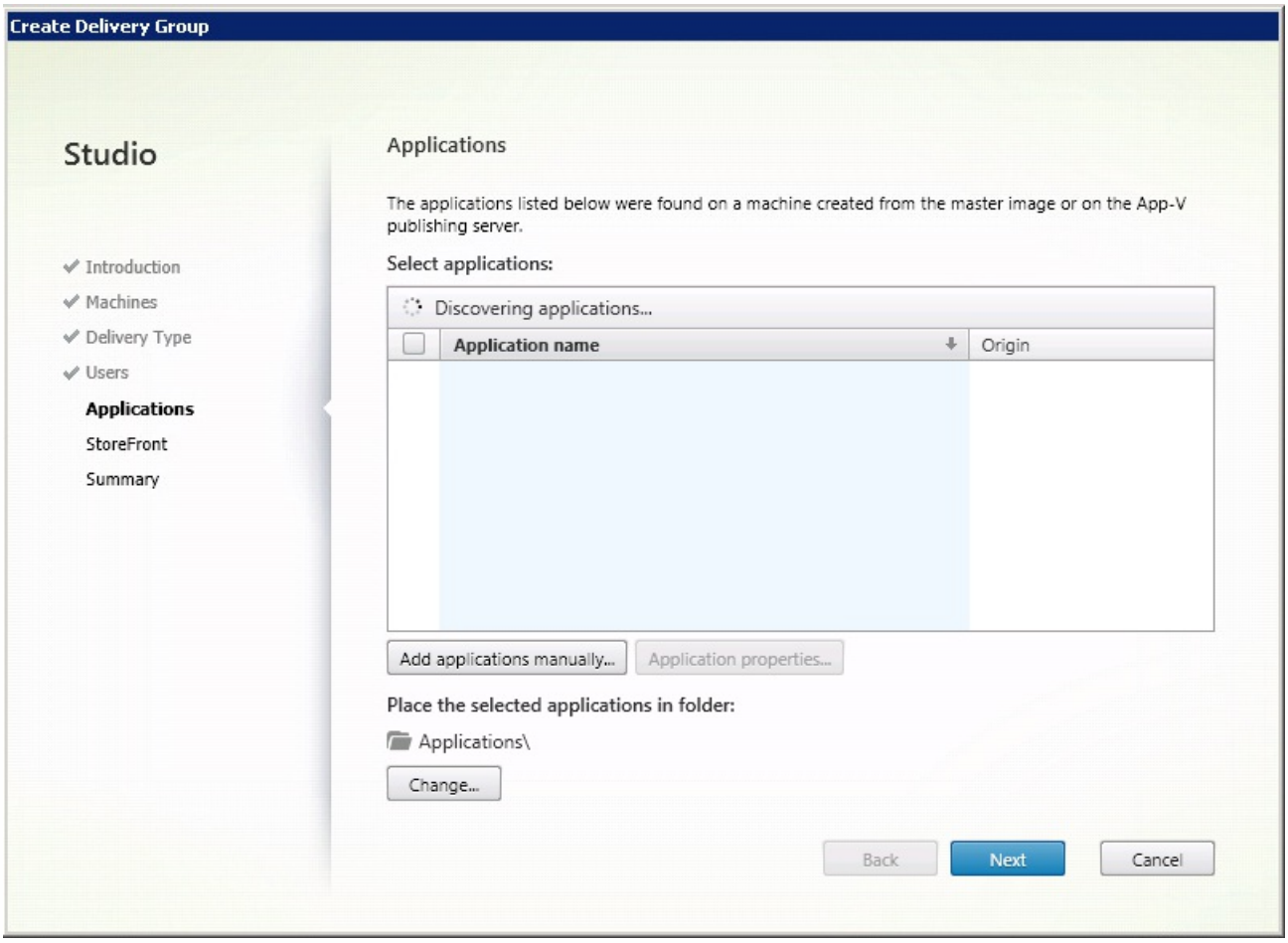
Application changes might not take effect for current application users until they log off their sessions.

By default, applications you add are placed in a folder named *— Applications*. You can:



- Create additional folders and then move applications into those new folders.
  - Folders can be nested up to five levels.
  - Folders do not have to contain applications; empty folders are allowed.
  - Folders are listed alphabetically unless you move them or specify a different location when you create them.
  - You can have more than one folder with the same name, as long as each has a different parent folder. Similarly, you can have more than one application with the same name, as long as each is in a different folder.
- Move a folder to the same or a different level. Moving is easiest using drag-and-drop.
- Rename or delete a folder you created. You cannot rename or delete the Applications folder, but you can move all the applications it contains to other folders you create.

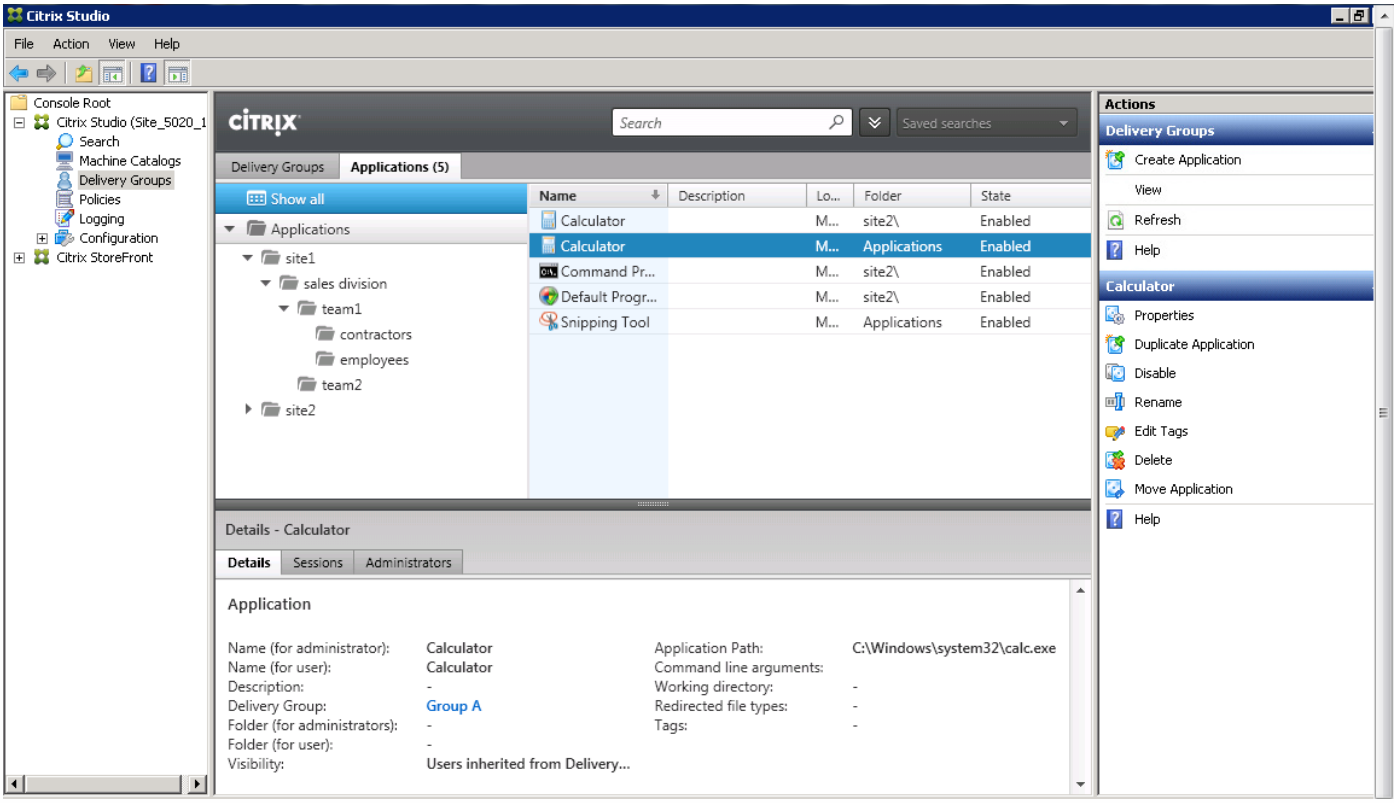
You can also create folders for applications when you create a Delivery Group.



You must have View Applications permission to see the applications in folders, and you must have Edit Application Properties permission for all applications in the folder to remove, rename, or delete a folder that contains applications. For details, see Delegated Administration.

Tip: The following instructions use the Actions pane in Studio. Alternatively, you can use right-click menus or drag and drop. If you create or move a folder in a location you did not intend, you can drag and drop it to the correct location.
Select Delivery Groups in the Studio navigation pane, and then select the Applications tab in the middle pane.

- To view all folders (excluding nested folders), click Show all.



- To create a folder:
  1. To place the new folder at the highest level (not nested under another folder), select the top Applications folder. To place the new folder under an existing folder other than Applications, select that folder.
  2. Select Create Folder in the Actions pane. Enter a 1-64 character name for the folder. Spaces are permitted.
- To move a folder:
  1. Select the folder and then select Move Folder in the Actions pane. (You can move only one folder at a time unless the folder contains nested folders.)
  2. To move the folder to the highest level (not nested under another folder), select the top Applications folder. To move a new folder under an existing folder other than Applications, select that folder.
- To rename a folder, select the folder, and then select Rename Folder in the Actions pane. Enter a 1-64 character new name.
- To delete a folder, select the folder, and then select Delete Folder in the Actions pane. When you delete a folder that contains applications and other folders, those objects are also deleted. Deleting an application removes the application assignment from the Delivery Group; it does not remove it from the machine.
- To move applications into a folder, select one or more applications, and then select Move Application in the Actions pane. Select the folder.

To add or move applications to folders from within the Create Delivery Group wizard, select one or more applications on the Applications page, and then select Change.

- To move the application to an existing folder, select that folder.
- To move the application to a new folder:
  - To create a folder at the highest level (not nested under another folder), select the top Applications folder and then select New folder. Specify a 1-64 character folder name. Spaces are allowed.
  - To create a new nested folder under an existing folder (other than Applications), select an existing folder and then select New folder. Specify a 1-64 character folder name. Spaces are allowed.

Users

Sep 30, 2014

There are two types of users: authenticated and unauthenticated (unauthenticated is also called anonymous). You can configure one or both types.

- **Authenticated** - The users and group members you specify by name must present credentials (such as smart card or user name and password) to StoreFront or Citrix Receiver to access applications and desktops.
- **Unauthenticated (anonymous)** - For Delivery Groups containing Server OS machines, you can select a check box that will allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. For example, when users access applications through kiosks, the application might require credentials, but the Citrix access portal and tools do not. An Anonymous Users Group is created when you install the VDA.
  - To grant access to unauthenticated users, each machine in the Delivery Group must have a VDA for Windows Server OS (minimum version 7.6) installed. When unauthenticated users are enabled, you must have an unauthenticated StoreFront store.
  - Unauthenticated user accounts are created on demand when a session is launched, and named AnonXYZ, in which XYZ is a unique three-digit value.
  - Unauthenticated user sessions have a default idle timeout of 10 minutes, and are logged off automatically when the client disconnects. Reconnection, roaming between clients, and Workspace Control are not supported.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane.
3. The following table describes your choices.

Enable access for	Add/assign users and user groups?	Enable the "Give access to unauthenticated users" check box?
Only authenticated users	Yes	No
Only unauthenticated users	No	Yes
Both authenticated and unauthenticated users	Yes	Yes

For Desktop Groups containing Desktop OS machines, you can import user data (a list of users) after you create the Delivery Group. See Import or export user lists below.

For Delivery Groups containing physical Desktop OS machines, you can import user information from a .csv file after you create the Delivery Group. You can also export user information to a .csv file. The .csv file can contain data from a previous product version.

The first line in the .csv file must contain comma-separated column headings (in any order), which can include: ADComputerAccount, AssignedUser, VirtualMachine, and HostId. Subsequent lines in the file contain comma-separated data. The ADComputerAccount entries can be common names, IP addresses, distinguished names, or domain and computer

name pairs.

To import or export user information:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane.
3. On the Machine Allocation page, select the Import list or Export list button, and then browse to the file location.

Sessions

Jul 29, 2016

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group and then select View Machines in the Actions pane.
3. To log a user off a session, select the session or desktop and select Log off in the Actions pane. The session closes and the machine becomes available to other users, unless it is allocated to a specific user.
   To disconnect a session, select the session or desktop, and select Disconnect in the Actions pane. Applications continue to run and the machine remains allocated to that user. The user can reconnect to the same machine.

   To send a message to users, select the session, machine, or user, and then select Send message in the Actions pane. Enter the message.

You can configure power state timers for Desktop OS machines to automatically handle unused sessions. See Power manage machines for details.

Note: These features are supported on Server OS machines only.

The session prelaunch and session linger features help specified users access applications quickly, by starting sessions before they are requested (session prelaunch) and keeping application sessions active after a user closes all applications (session linger).

By default, session prelaunch and session linger are not used: a session starts (launches) when a user starts an application, and remains active until the last open application in the session closes.

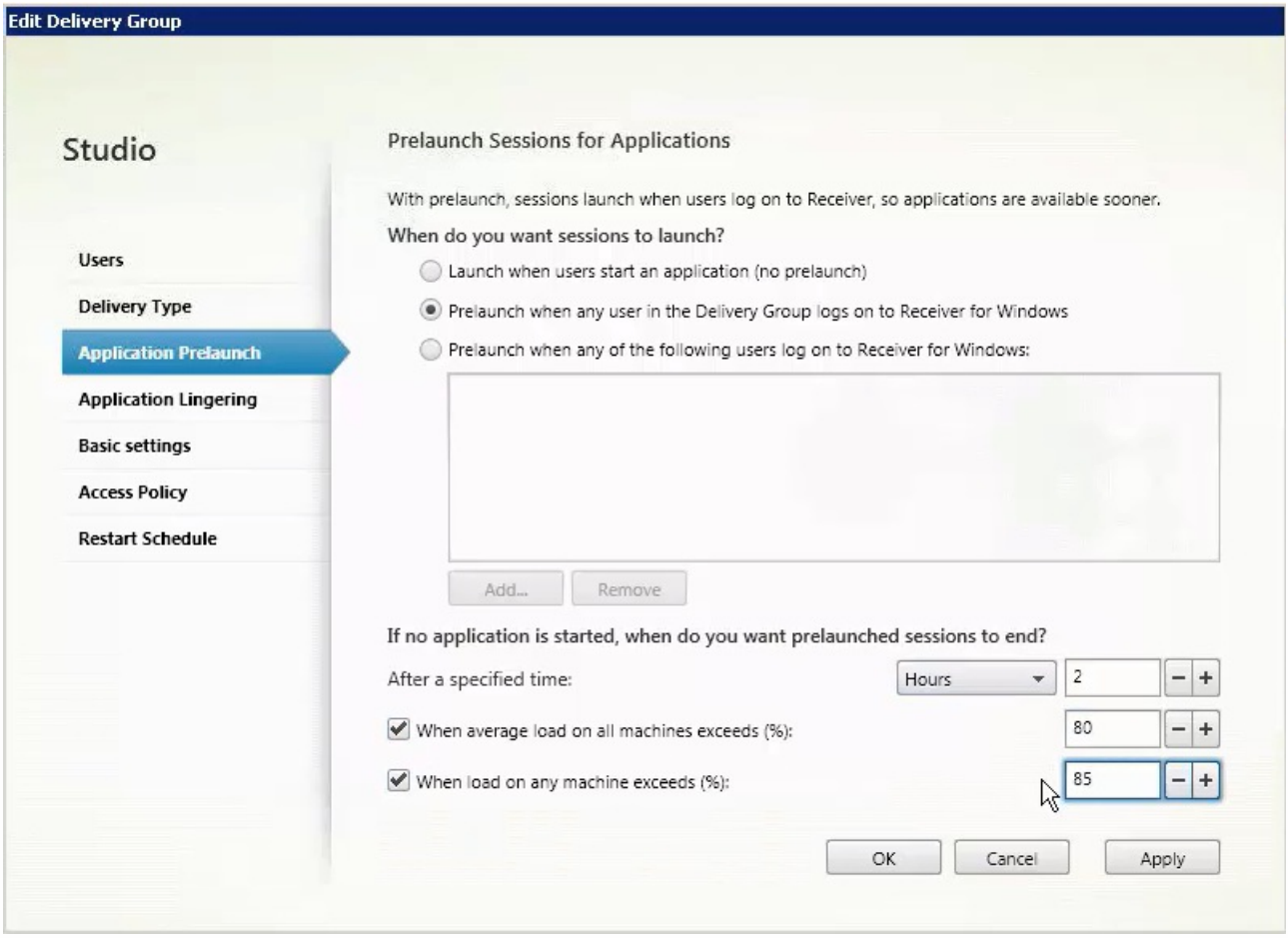
Considerations:

- The Delivery Group must support applications, and the machines must be running a VDA for Server OS, minimum version 7.6.
- Session prelaunch is supported only when using Citrix Receiver for Windows. Session linger is supported when using Citrix Receiver for Windows and Receiver for Web. Additional Receiver configuration is required. For instructions, search for “session prelaunch” in the eDocs content for your Receiver for Windows version.
  Note: Receiver for HTML5 is not supported.
- When using session prelaunch:
  - Regardless of the admin-side settings, if an end user’s machine is put into "suspend" or "hibernate" mode, prelaunch

will not work.
    - Prelaunch will work as long as the end user locks their machine/session, but if the end user logs off from Citrix Receiver, the session is ended and prelaunch no longer applies.
- Prelaunched and lingering sessions consume a license, but only when connected. Unused prelaunched and lingering sessions disconnect after 15 minutes by default. This value can be configured in PowerShell (New/Set-BrokerSessionPreLaunch cmdlet).
- Careful planning and monitoring of your users' activity patterns are essential to tailoring these features to complement each other. Optimal configuration balances the benefits of earlier application availability for users against the cost of keeping licenses in use and resources allocated.
- You can also configure session prelaunch for a scheduled time of day in Receiver.

To enable session prelaunch:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then click Edit Delivery Group in the Actions pane.
3. On the Application Prelaunch page, enable session prelaunch by choosing when sessions should launch:
    - When a user starts an application. This is the default setting; session prelaunch is disabled.
    - When any user in the Delivery Group logs on to Receiver for Windows.
    - When anyone in a list of users and user groups logs on to Receiver for Windows. Be sure to also specify users or user groups if you choose this option.



4. A prelaunched session is replaced with a regular session when the user starts an application. If the user does not start an application (the prelaunched session is unused), the following settings affect how long that session remains active. For

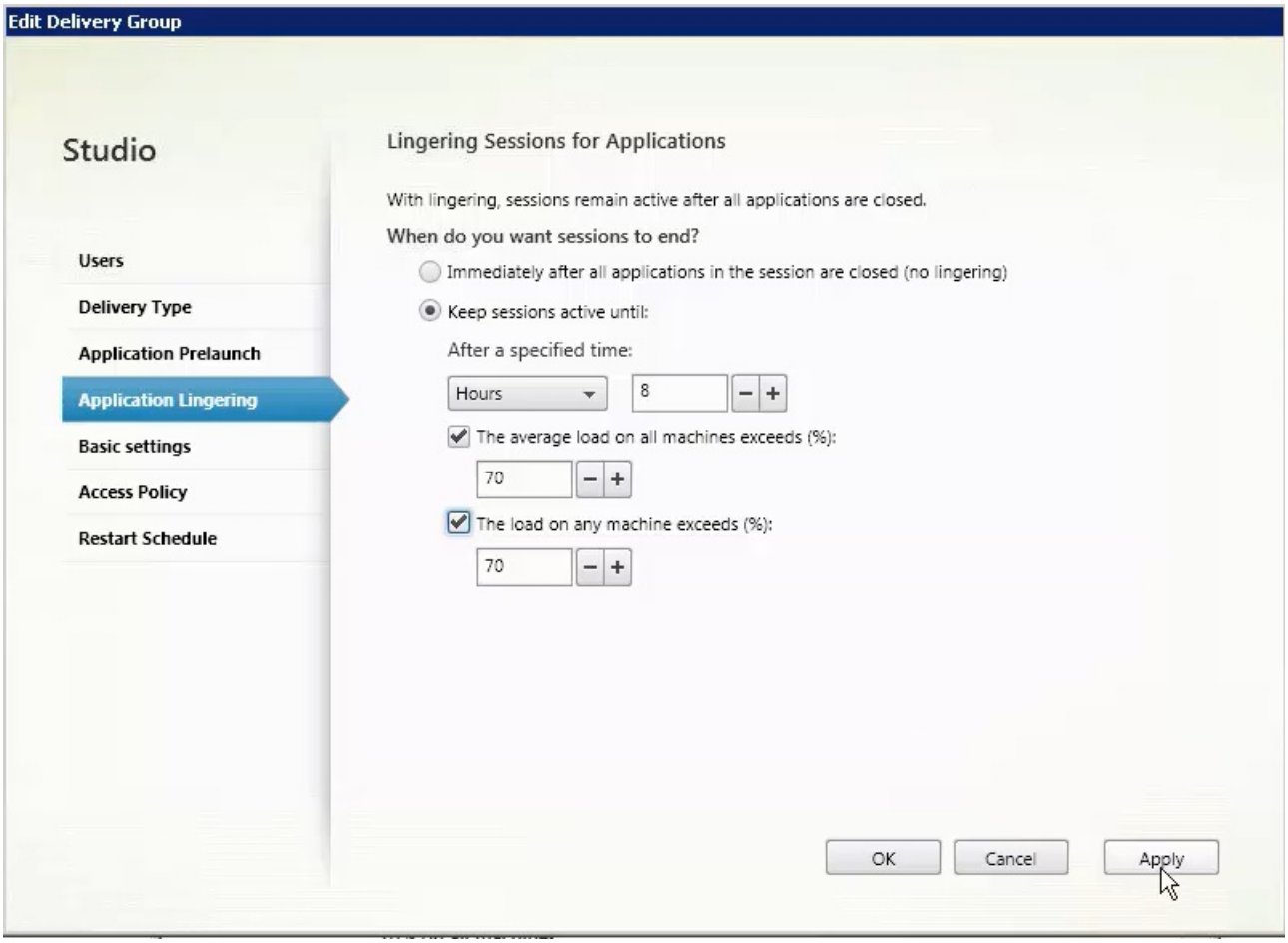
details about these settings, see
— How long unused prelaunched and lingering sessions remain active
below.

- When a specified time interval elapses. You can change the time interval (1-99 days, 1-2376 hours, or 1-142,560 minutes).
- When the average load on all machines in the Delivery Group exceeds a specified percentage (1-99%).
- When the load on any machine in the Delivery Group exceeds a specified percentage (1-99%).

Recap: A prelaunched session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

To enable session linger:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then click Edit Delivery Group in the Actions pane.
3. On the Application Lingering page, enable session linger by selecting the Keep sessions active until radio button.



4. Several settings affect how long a lingering session remains active if the user does not start another application. For details about these settings, see
— How long prelaunched and lingering sessions remain active
below.

- When a specified time interval elapses. You can change the time interval (1-99 days, 1-2376 hours, or 1-142,560 minutes).
- When the average load on all machines in the Delivery Group exceeds a specified percentage (1-99%).
- When the load on any machine in the Delivery Group exceeds a specified percentage (1-99%).

Recap: A lingering session remains active until one of the following events occurs: a user starts an application, the

specified time elapses, or a specified load threshold is exceeded.

How long unused prelaunched and lingering sessions remain active - There are several ways to specify how long an unused session remains active if the user does not start an application: a configured timeout and server load thresholds. You can configure all of them; the event that occurs first will cause the unused session to end.

- Timeout - A configured timeout specifies the number of minutes, hours, or days an unused prelaunched or lingering session remains active. If you configure too short a timeout, prelaunched sessions will end before they provide the user benefit of quicker application access. If you configure too long a timeout, incoming user connections might be denied because the server doesn't have enough resources.
  You cannot disable this timeout from Studio, but you can in the SDK (New/Set-BrokerSessionPreLaunch cmdlet). If you disable the timeout, it will not appear in the Studio display for that Delivery Group or in the Edit Delivery Group wizard.

- Thresholds - Automatically ending prelaunched and lingering sessions based on server load ensures that sessions remain open as long as possible, assuming server resources are available. Unused prelaunched and lingering sessions will not cause denied connections because they will be ended automatically when resources are needed for new user sessions.
  You can configure two thresholds: the average percentage load of all servers in the Delivery Group, and the maximum percentage load of a single server in the Delivery Group. When a threshold is exceeded, the sessions that have been in the prelaunch or lingering state for the longest time are ended, sessions are ended one-by-one at minute intervals until the load falls below the threshold. (While the threshold is exceeded, no new prelaunch sessions are started.)

Servers with VDAs that have not registered with the Controller, and servers in maintenance mode are considered fully loaded. An unplanned outage will cause prelaunch and lingering sessions to be ended automatically to free capacity.

XenApp published apps and desktops

Sep 09, 2015

Use Server OS machines to deliver XenApp published apps and XenApp published desktops.

This table describe the situations, users, and considerations for using these delivery methods.

Use Case	**You want** Inexpensive server-based delivery to minimize the cost of delivering applications to a large number of users, while providing a secure, high-definition user experience. **Your users** Perform well-defined tasks and do not require personalization or offline access to applications. Users may include task workers such as call center operators and retail workers, or users that share workstations. **Application types** Any application.
Benefits and considerations	**Benefits** Manageable and scalable solution within your datacenter. Most cost effective application delivery solution. Hosted applications are managed centrally and users cannot modify the application, providing a user experience that is consistent, safe, and reliable. **Considerations** Users must be online to access their applications.
User experience	User requests one or more applications from StoreFront, their Start menu, or a URL you provide to them. Applications are delivered virtually and display seamlessly in high definition on user devices. Depending on profile settings, user changes are saved when the user's application session ends. Otherwise, the changes are deleted.
Process, host, and deliver applications	**Process** Application processing takes place on hosting machines, rather than on the user devices. The hosting machine can be a physical or a virtual machine. **Host**

	Applications and desktops reside on a Server OS machine. Machines become available through machine catalogs. **Delivery** Machines within machine catalogs are organized into Delivery groups that deliver the same set of applications to groups of users. Server OS machines support: • Desktop and applications Delivery groups that host both desktops and applications. • Application Delivery groups that host only applications.
Session management and assignment	**Sessions** Server OS machines run multiple sessions from a single machine to deliver multiple applications and desktops to multiple, simultaneously connected users. Each user requires a single session from which they can run all their hosted applications. For example, a user logs on and requests an application. One session on that machine becomes unavailable to other users. A second user logs on and requests an application which that machine hosts. A second session on the same machine is now unavailable. If both users request additional applications, no additional sessions are required because a user can run multiple application using the same session. If two more users log on and request desktops, and two sessions are available on that same machine, that single machine is now using four sessions to host four different users. **Random machine assignments** Within the Delivery group to which a user is assigned, a machine on the least loaded server is selected. A machine with session availability is randomly assigned to deliver applications to a user when that user logs on.

To deliver XenApp published apps:

1. Install the applications you want to deliver on a master image running a supported Windows server OS.
2. Create a machine catalog for this master image or update an existing catalog with the master image.
3. Create an application Delivery group to deliver the application to users.
4. From the list of application installed, select the application you want to deliver.

To deliver XenApp published desktops:

1. Install apps on a master image running a supported Windows server OS.
2. Create a machine catalog for this master image or update an existing catalog with the master image.
3. Create a desktop Delivery group to deliver the desktops to users.

VM hosted apps

Sep 09, 2015

Use Desktop OS machines to deliver VM hosted app.

This table describe the situations, users, and considerations for using this delivery method.

Use Case	**You want** A client-based application delivery solution that is secure, provides centralized management, and supports a large number of users per host server (or hypervisor), while providing users with applications that display seamlessly in high-definition. **Your users** Are internal, external contractors, third-party collaborators, and other provisional team members. Your users do not require off line access to hosted applications. **Application types** Applications that might not work well with other applications or might interact with the operation system, such as Microsoft .NET framework. These types of applications are ideal for hosting on virtual machines. Applications running on older operating systems such as Windows XP or Windows Vista, and older architectures, such as 32-bit or 16-bit. By isolating each application on its own virtual machine, if one machine fails, it does not impact other users.
Benefits and considerations	**Benefits** Applications and desktops on the master image are securely managed, hosted, and run on machines within your datacenter, providing a more cost effective application delivery solution. • On log on, users can be randomly assigned to a machine within a Delivery Group that is configured to host the same application. • You can also statically assign a single machine to deliver an application to a single user each time that user logs on. Statically assigned machines allow users to install and manage their own applications on the virtual machine. **Considerations** Running multiple sessions is not supported on Desktop OS machines. Therefore, each user consumes a single machine within a Delivery group when they log on, and users must be online to access their applications. This method may increase the amount of server resources for processing applications and increase the amount of storage for users' Personal vDisks.
User	The same seamless application experience as hosting shared applications on Server OS machines.

experience	
Process, host, and deliver applications	**Process** The same as Server OS machines except they are virtual Desktop OS machines. **Host** The same as Server OS machines except they are virtual Desktop OS machines. **Delivery** The same as Server OS machines except Desktop OS machines can exist only in a desktop Delivery group.
Session management and assignment	**Sessions** Desktop OS machines run a single desktop session from a single machine. When accessing applications only, a single user can use multiple applications (and is not limited to a single application) because the operating system sees each application as a new session. **Random and static machine assignments** Within a Delivery group to which a user is assigned, when users log on they can access: ● Statically assigned machine so that each time the user logs on to the same machine. ● Randomly assigned machine that is selected based on session availability.

To deliver VM hosted apps:

1. Install the applications you want to deliver on a master image running a supported Windows desktop OS.
2. Create a machine catalog for this master image or update an existing catalog with the master image.
   When defining the desktop experience for the machine catalog, decide whether you want users to connect to a new VM each time they log in or connect to the same machine each time they log in.
3. Create an application Delivery group to deliver the application to users.
4. From the list of application installed, select the application you want to deliver.

VDI desktops

Sep 09, 2015

Use Desktop OS machines to deliver VDI desktops.

VDI desktops are hosted on virtual machines and provide each user with a desktop operating system.

VDI desktops require more resources than XenApp published desktops, but do not require that applications installed on them support server-based operating systems. In additional, depending on the type of VDI desktop you choose, these desktop can be assigned to individual users and allow these users a high degree of personalization.

When you create a machine catalog for VDI desktops, you create one of these types of desktops:

- Random non-persistent desktops, also known as Pooled VDI desktops. Each time a users logs on to use one of these desktops, they connect to a dynamically selected desktop in a pool of desktops based on a single master image. All changes to the desktop are lost when the machine reboots.
- Static non-persistent desktop. The first time a user logs on the use one off these desktops, the user is assigned a desktop from a pool of desktops based on a single master image. After the first use, each time a user logs in to use one of these desktop, the user connects to the same desktop that user was assigned on first use. All changes to the desktop are lost when the machine reboots.
- Static persistent, also known as VDI with Personal vDisk. Unlike other types of VDI desktops, these desktops can be fully personalized by users. The first time a user logs on the use one off these desktops, the user is assigned a desktop from a pool of desktops based on a single master image. After the first use, each time a user logs in to use one of these desktop, the user connects to the same desktop that user was assigned on first use. Changes to the desktop are retained when the machine reboots because they are stored in a Personal vDisk.

To deliver VDI desktops:

1. Create a master image running a supported Windows desktop OS.
2. Create a machine catalog for this master image or update an existing catalog with the master image.
   When defining the desktop experience for the machine catalog, decide whether you want users to connect to a new VM each time the log in or connect to the same machine each time they log in and specify how changes to the desktop are retained.
3. Create a desktop Delivery group to deliver the desktops to users.

Remote PC Access

Aug 10, 2016

Remote PC Access allows an end user to log on remotely from virtually anywhere to the physical Windows PC in the office. The Virtual Delivery Agent (VDA) is installed on the office PC; it registers with the Delivery Controller and manages the HDX connection between the PC and the end user client devices. Remote PC Access supports a self-service model; after you set up the whitelist of machines that users are permitted to access, those users can join their office PCs to a Site themselves, without administrator intervention. The Citrix Receiver running on their client device enables access to the applications and data on the office PC from the Remote PC Access desktop session.

A user can have multiple desktops, including more than one physical PC or a combination of physical PCs and virtual desktops.

Note: Sleep mode & Hibernation mode for Remote PC is not supported. Remote PC Access is valid only for XenDesktop licenses; sessions consume licenses in the same way as other XenDesktop sessions.
Active Directory considerations:

- Before configuring the remote PC deployment site, set up your Organizational Units (OUs) and security groups and then create user accounts. Use these accounts to specify users for the Delivery Groups you will use to provide Remote PC Access.
- If you modify Active Directory after a machine has been added to a machine catalog, Remote PC Access does not reevaluate that assignment. You can manually reassign a machine to a different catalog, if needed.
- If you move or delete OUs, those used for Remote PC Access can become out of date. VDAs might no longer be associated with the most appropriate (or any) machine catalog or Delivery Group.

Machine catalog and Delivery Group considerations:

- A machine can be assigned to only one machine catalog and one Delivery Group at a time.
- You can put machines in one or more Remote PC Access machine catalogs.
- When choosing Machine Accounts for a machine catalog, select the lowest applicable OU to avoid potential conflicts with machines in another catalog. For example, in the case of Bank/officers/tellers, select tellers.
- You can allocate all machines from one remote PC machine catalog through one or more Delivery Groups. For example, if one group of users requires certain policy settings and another group requires different settings, assigning the users to different Delivery Groups enables you to filter the HDX policies according to each Delivery Group.
- If your IT infrastructure assigns responsibility for servicing users based on geographic location, department, or some other category, you can group machines and users accordingly to allow for delegated administration. Ensure that each administrator has permissions for both the relevant machine catalogs and the corresponding Delivery Groups.
- For users with office PCs running Windows XP, create a separate machine catalog and Delivery Group for those systems. When choosing machine accounts for that catalog in Studio, select the checkbox indicating that some machines are running Windows XP.

Deployment considerations:

- You can create a Remote PC Access deployment and then add traditional Virtual Desktop Infrastructure (VDI) desktops or applications later. You can also add Remote PC Access desktops to an existing VDI deployment.
- Consider whether to enable the Windows Remote Assistance feature when you install the VDA on the office PC. This option allows help desk teams using Director to view and interact with a user sessions using Windows Remote Assistance.
- Consider how you will deploy the VDA to each office PC. Citrix recommends using electronic software distribution such as Active Directory scripts and Microsoft System Center Configuration Manager. The installation media contains sample

Active Directory scripts.

- Secure Boot functionality is currently unsupported. Disable Secure Boot if intending to deploy the workstation VDA.
- Each office PC must be domain-joined with a wired network connection.
- Windows 7 Aero is supported on the office PC, but not required.
- Connect the keyboard and mouse directly to the PC or laptop, not to the monitor or other components that can be turned off. (If you must connect input devices to components such as monitors, they should not be turned off.)
- If you are using smart cards, see Smart cards.
- Remote PC Access can be used on most laptop computers. To improve accessibility and deliver the best connection experience, configure the laptop power saving options to those of a desktop PC. For example:
  - Disable the Hibernate feature.
  - Disable the Sleep feature.
  - Set the close lid action to Do Nothing.
  - Set the press the power button action to Shut Down.
  - Disable video card energy saving features.
  - Disable network interface card energy saving features.
  - Disable battery saving technologies.

  The following are not supported for Remote PC Access devices:

  - Docking and undocking the laptop.
  - KVM switches or other components that can disconnect a session.
  - Hybrid PCs (including All-in-One and NVIDIA Optimus laptops and PCs) and Surface Pro/Books.
- Install Citrix Receiver on each client device that remotely accesses the office PC.
- Multiple users with remote access to the same office PC see the same icon in Receiver. When any user remotely logs on to the PC, that resource appears as unavailable to other users.
- By default, a remote user's session is automatically disconnected when a local user initiates a session on that machine (by pressing CTRL+ATL+DEL). To prevent this automatic action, add the following registry entry on the office PC, and then restart the machine.
  Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.
  HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001

  To further customize the behavior of this feature under HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC

  • RpcaMode (dword)

  • RpcaTimeout (dword)

  RpcaMode:

  1 - Means that the remote user will always win if he does not respond to the Messaging UI in the specified timeout period.

  2 - Means that the Local user will always win. If this setting is not specified, the Remote user will always win by default.

  RpcaTimeout:

  The number of seconds given to the user before we automatically decide which type of mode to enforce. If this setting is not specified, the default value is :30 seconds. The minimum value here should be :30 seconds. The User needs to restart the machine for these changes to take place.

When user wants to forcibly get the console access: The local user can hit Ctr+Alt+Del twice in a gap of :10 seconds to get local control over a remote session and force a disconnect event.

After the registry change and machine restart, if a local user presses CTRL+ALT+DEL to log on to that PC while it is in use by a remote user, the remote user receives a prompt asking whether or not to allow or deny the local user's connection. Allowing the connection will disconnect the remote user's session.

The following XenDesktop features are not supported for Remote PC Access deployments:

- Creating master images and virtual machines
- Delivering hosted applications
- Personal vDisks
- Client folder redirection

Remote PC Access supports Wake on LAN, which gives users the ability to turn on physical PCs remotely. This feature enables users to keep their office PCs turned off when not in use, saving energy costs. It also enables remote access when a machine has been turned off inadvertently, such as during weather events.

With XenDesktop 7.6 Feature Pack 3, Citrix released an experimental Wake on LAN SDK. This enables you or a third-party Wake on LAN solution to create a connector without the requirement of System Center 2012 R2. For more information, see http://support.citrix.com/article/CTX202272.

The Remote PC Access Wake on LAN feature is supported on both of the following:

- PCs that support Intel Active Management Technology (AMT)
- PCs that have the Wake on LAN option enabled in the BIOS

You must configure Microsoft System Center Configuration Manager (ConfigMgr) 2012 to use the Wake on LAN feature. ConfigMgr provides access to invoke AMT power commands for the PC, plus Wake-up proxy and magic-packet support. Then, when you use Studio to create a Remote PC Access deployment (or when you add another power management connection to be used for Remote PC Access), you enable power management and specify ConfigMgr access information.

Additionally:

- Using AMT power operations is preferred for security and reliability; however, support is also provided for two non-AMT methods: ConfigMgr Wake-up proxy and raw magic packets.
- On AMT-capable machines only, the Wake on LAN feature also supports the Force-Shutdown and Force-Restart actions in Studio and Director. Additionally, a Restart action is available in StoreFront and Receiver.

For more information, see Configuration Manager and Remote PC Access Wake on LAN and Provide users with Remote PC Access.

Provide users with Remote PC Access

Jun 30, 2014

Using Remote PC Access, desktop users can securely access resources on the office PC while experiencing the benefits of Citrix HDX technology.

Note: Remote PC Access is valid only for XenDesktop licenses.

1. To use the Remote PC Access power management feature (also known as Remote PC Access Wake on LAN), complete the configuration tasks on the PCs and on Microsoft System Center Configuration Manager (ConfigMgr) before creating the Remote PC Access deployment in Studio. See Configuration Manager and Remote PC Access Wake on LAN for details.
2. When creating the initial Remote PC Access deployment, you can enable or disable power management for the machines in the default Remote PC Access Machine Catalog. If you enable power management, specify ConfigMgr connection information. Then specify users and machine accounts. See Create a Site for more information. Creating a Remote PC deployment does not prevent VDI use of the Site in the future.
   Creating a Remote PC Access deployment creates a default machine catalog named
   — Remote PC Access Machines
   and a default delivery group named
   — Remote PC Access Desktops
   .
3. When creating another machine catalog for use with Remote PC Access:
   - Operating System: Select Remote PC Access, and choose a power management connection. You can also choose not to use power management. If there are no configured power management connections, you can add one after you finish the machine catalog creation wizard (connection type = Microsoft Configuration Manager Wake on LAN), and then edit the machine catalog, specifying that new connection.
   - Machine Accounts: You can select from the machine accounts or Organizational Units (OUs) displayed, or add machine accounts and OUs.
4. Install the VDA on the office PC used for local and remote access. Typically, you deploy the VDA automatically using your package management software; however, for proof-of-concept or small deployments, you can install the VDA manually on each office PC.
   After the VDA is installed, the next domain user that logs on to a console session (locally or through RDP) on the office PC is automatically assigned to the Remote PC desktop. If additional domain users log on to a console session, they are also added to the desktop user list, subject to any restrictions you have configured.
   Note: To use RDP connections outside of your XenApp or XenDesktop environment, you must add users or groups to the Direct Access Users group.
5. Instruct users to download and install Citrix Receiver onto each client device they will use to access the office PC remotely. Citrix Receiver is available from http://www.citrix.com or the application distribution systems for supported mobile devices.

You can edit a power management connection to configure advanced settings. You can enable:

- Wake-up proxy delivered by ConfigMgr.
- Wake on LAN (magic) packets. If you enable Wake on LAN packets, you can select a Wake on LAN transmission method: subnet-directed broadcasts or Unicast.

The PC uses AMT power commands (if they are supported), plus any of the enabled advanced settings. If the PC does not use AMT power commands, it uses the advanced settings.

The Delivery Controller writes the following diagnostic information about Remote PC Access to the Windows Application Event log. Informational messages are not throttled. Error messages are throttled by discarding duplicate messages.

- 3300 (informational) - Machine added to catalog
- 3301 (informational) - Machine added to delivery group
- 3302 (informational) - Machine assigned to user
- 3303 (error) - Exception

When power management for Remote PC Access is enabled, subnet-directed broadcasts might fail to start machines that are located on a different subnet from the Controller. If you need power management across subnets using subnet-directed broadcasts, and AMT support is not available, try the Wake-up proxy or Unicast method (ensure those settings are enabled in the advanced properties for the power management connection).

Manage Remote PC Access Delivery Groups

Jun 02, 2014

If a machine in a Remote PC Access machine catalog is not assigned to a user, Studio temporarily assigns the machine to a Delivery Group associated with that machine catalog. This temporary assignment provides information, so that the machine can be assigned later to a user. The Delivery Group to machine catalog association has a priority value.

Priority determines to which Delivery Group that machine is assigned when it registers with the system or when a user needs a machine assignment. The lower the value, the higher the priority. If a Remote PC Access machine catalog has multiple Delivery Group assignments, the software selects the match with the highest priority. You can set this priority value using the PowerShell SDK.

When first created, Remote PC Access machine catalogs are associated with a Delivery Group. This means that machine accounts or Organizational Units added to the machine catalog later can be added to the Delivery Group. This association can be switched off or on.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Remote PC Access Delivery Group.
3. In the Details section, select the Catalogs tab and then select a Remote PC Access machine catalog.
4. To add or restore an association, select Add Desktops. To remove an association, select Remove Association.

App-V

Nov 02, 2015

Microsoft Application Virtualization (App-V) lets you deploy, update, and support applications as services. Users access applications without installing them on their own devices. App-V and Microsoft User State Virtualization (USV) provide access to applications and data, regardless of location and connection to the Internet.

The following table lists supported versions. (The App-V 4.6 2 client is no longer supported.)

App-V	XenDesktop and XenApp versions	
	Delivery Controller	VDA
5.0	XenDesktop 7 through current XenApp 7.5 through current	7.0 through current
5.0 SP1	XenDesktop 7 through current XenApp 7.5 through current	7.0 through current
5.0 SP2	XenDesktop 7 through current XenApp 7.5 through current	7.1 through current
5.0 SP3 and 5.1	XenDesktop 7.6 XenApp 7.6	7.6.300

The supported App-V client does not support offline access to applications. App-V integration support includes using SMB shares for applications; the HTTP protocol is not supported.

Applications are available seamlessly without any pre-configuration or changes to operating system settings. App-V contains the following components:

- Management server — Provides a centralized console to manage App-V infrastructure and deliver virtual applications to both the App-V Desktop Client as well as a Remote Desktop Services Client. The App-V management server authenticates, requests, and provides the security, metering, monitoring, and data gathering required by the administrator. The server uses Active Directory and supporting tools to manage users and applications.
- Publishing server — Provides App-V clients with applications for specific users, and hosts the virtual application package for streaming. It fetches the packages from the management server.
- Client — Retrieves virtual applications, publishes the applications on the client, and automatically sets up and manages virtual environments at runtime on Windows devices. The App-V client is installed on the VDA and stores user-specific virtual application settings, such as registry and file changes in each user's profile.

You can launch App-V applications from Server OS and Desktop OS Delivery Groups:

- Through Citrix Receiver
- From the Start menu
- Through the App-V client and Citrix Receiver
- Simultaneously by multiple users on multiple devices
- Through Citrix StoreFront

Modified App-V application properties are implemented when the application is started. For example, for applications with a modified display name or customized icon, the modification appears when users start the application.

There is no change in App-V applications performance when a desktop and application Delivery Group is changed to an application-only Delivery Group.

Only an App-V server-based deployment in which an administrator uses an App-V management server and publishing server to manage App-V applications is supported.

To deliver App-V applications:

1. Deploy App-V, as described in the instructions in http://technet.microsoft.com/en-us/virtualization/hh710199.
2. Publish the App-V applications on the App-V management server. Configure settings such as permissions and File Type Association. These settings already exist if you already deployed App-V.
3. Optionally, change App-V publishing server settings; see below.
4. Install the App-V client on VDAs.
5. During Site creation in Studio, specify the App-V publishing and management server URLs with port numbers. These servers are automatically used by the Delivery Groups.
6. Install the App-V client in the master image for machine catalogs. Configured the client with settings such as ShareContentStoreMode and EnablePackageScripts. (You do not need to configure the App-V Publishing Server in the master image because it is configured during application launch.)
7. During Delivery Group creation, select the App-V applications.

The applications are now available.

You can specify or change App-V server information after you create a Site. Select Configuration > App-V Publishing in the Studio navigation pane and then selecting entries in the Actions pane. You can add App-V publishing by specifying URLs with port numbers for the App-V management and publishing servers. You can also edit or remove those addresses. If you refresh the App-V applications, the display indicates if there is a problem connecting to a server and removes entries for applications that are no longer available.

To change publishing server settings, Citrix recommends using the SDK cmdlets on the Controller.

- To view publishing server settings, enter Get-CtxAppvServerSetting -AppVPublishingServer <pubServer>.
- To ensure that App-V applications launch properly, enter Set-CtxAppvServerSetting –UserRefreshonLogon 0.

The following cmdlet changes the settings of the App-V publishing server on the Controller. Not all parameters are mandatory.

```
Set-CtxAppvServerSetting –AppVPublishingServer
<pubServer> -UserRefreshOnLogon <bool> -UserRefrehEnabled <bool>
-UserRefreshInterval <int> -UserRefreshIntervalUnit <Day/Hour>
-GlobalRefreshOnLogon <bool> -GlobalRefresfEnabled<bool>
-GlobalRrefreshInterval <int> -GlobalRefreshIntervalUnit <Day/Hour>
```

Note: If you previously used GPO policy settings for managing publishing server settings, the GPO settings override any App-V integration settings, including the previous cmdlet settings. This may result in App-V application launch failure. Citrix recommends that you remove all GPO policy settings and configure the same settings using the SDK.

- If the Test connection operation returns an error when you specify App-V management server and publishing server addresses in Studio, check the following:
  1. The App-V server is powered on: either send a Ping command or check the IIS Manager (each App-V server should be in a Started and Running state).
  2. PowerShell remoting is enabled on the App-V server. If it is not, follow the procedure in http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
  3. The App-V server is added to Active Directory.
     If the Studio machine and the App-V server are in different Active Directory domains that do not have a trust relationship, from the PowerShell console on the Studio machine, run winrm s winrm/Config/client '@(TrustedHosts="<App-V server FQDN>")'. If TrustedHosts is managed by GPO, the following error message will display: "The config setting TrustedHosts cannot be changed because use is controlled by policies. The policy would need to be set to "Not Configured" in order to change the config setting". If this message displays, add an entry for the App-V server name to the TrustedHosts policy in GPO (Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Client).
  4. The Studio administrator is also an App-V server administrator.
  5. File sharing is enabled on the App-V server: enter \\<App-V server FQDN> in Windows Explorer or with the Run command.
  6. The App-V server has the same file sharing permissions as the App-V administrator: on the App-V server, add an entry for\\<App-V Server FQDN> in Stored User Names and Passwords, specifying the credentials of the user who has administrator privileges on the App-V server. For guidance, see http://support.microsoft.com/kb/306541.
- If Application discovery fails, check the following:
  1. Studio administrator is an App-V management server administrator.
  2. The App-V management server is running. Check this by opening the IIS Manager; the server should be in a Started and Running state.
  3. PowerShell remoting is enabled on the App-V servers. If either is not enabled, follow the procedure in http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
  4. Packages have appropriate security permissions for the Studio administrator to access.
- If App-V applications do not launch, check the following:
  1. The publishing server is running. Check this by opening the IIS Manager; the server should be in a Started and Running state.
  2. App-V packages have appropriate security permissions so that users can access.
  3. On the VDA:
     - Make sure that Temp is pointing to the correct location, and that there is enough space available in the Temp directory.
     - Make sure that the App-V client is installed, and no earlier than version 5.0.
     - Make sure you have Administrator permissions and run Get-AppvClientConfiguration. Make sure that EnablePackageScripts is set to 1. If it is not set to 1, run Set-AppvClientConfiguration -EnablePackageScripts $true. Citrix recommends that you perform this step when you create a master image so that all VDAs created from the master image have the correct configuration.
     - From the Registry editor (regedit), go to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV. Make sure that the AppVServers key has the following value format: AppVManagementServer+metadata;PublishingServer (for example: http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082).
     - Make sure that CtxAppVCOMAdmin has administrator privileges. During VDA installation CtxAppVCOMAdmin is usually created and added to the Local Administrators Group on the VDA machine. However, depending on the Active Directory policy, this user might lose the administrative association.

Run compmgmt.msc and browse to Local Users and Groups Users. If CtxAppVCOMAdmin is not an administrator, edit the group policy or contact your administrator, so that this user account retains its administrative association.

4. On the master image where the App-V client is installed, the PowerShell ExecutionPolicy should be set to RemoteSigned because the AppV client module provided by Microsoft is not signed, and this ExecutionPolicy allows PowerShell to run unsigned local scripts and cmdlets. Use one of the following methods to set the ExecutionPolicy:
   - Logged in as administrator, enter the following PowerShell cmdlet: Set-ExecutionPolicy RemoteSigned.
   - From Group Policy settings, go to Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell> Turn on Script Execution.
5. Check the publishing servers:
   - Run Get-AppvPublishingServer * to display the list of publishing servers.
   - Check whether UserRefreshonLogon is set to False. If not, the first App-V application launch typically fails.
   - With Administrator privileges, run Set-AppvPublishingServer and set UserRefreshonLogon to False.

   If these steps do not resolve the issues, enable and examine the logs.

To enable Studio logs:

1. Create the folder C:\CtxAppvLogs.
2. Go to C:\ProgramFiles\Citrix\StudioAppVInegration\SnapIn\Citrix.Appv.Admin.V1 and open CtxAppvCommon.dll.config in a text editor such as Notepad, as an administrator. Uncomment the following line:
   <add key =”LogFileName” value=”C:\CtxAppvLogs\log.txt”/>

To enable VDA logs:

1. Create the folder C:\CtxAppvLogs.
2. Go to C:\ProgramFiles\Citrix\ Virtual Desktop Agent, and open CtxAppvCommon.dll.config in a text editor such as Notepad, as an administrator. Uncomment the following line:
   <add key =”LogFileName” value=”C:\CtxAppvLogs\log.txt”/>
3. Uncomment the following line and set the value field to 1, as shown in the following example:
   <add key =”EnableLauncherLogs” value=”1”/>

   All configuration-related logs are located at C:\CtxAppvLogs. The application launch logs are located at:
   - XenDesktop 7.1 and later, and XenApp 7.5 and later — %LOCALAPPDATA%\Citrix\CtxAppvLogs.
   - XenDesktop 7.0 — %LocalAppData%\temp\CtxAppVLogs

   LOCALAPPDATA resolves to the local folder for the logged in user. Make sure to check in the local folder of the launching user (for whom application launch failed).
4. As administrator, restart the Broker service or restart the VDA machine to start logging.

Local App Access and URL redirection

Sep 09, 2015

Local App Access seamlessly integrates locally installed Windows applications into a hosted desktop environment without changing from one computer to another. With Local App Access, you can:

- Access applications installed locally on a physical laptop, PC, or other device directly from the virtual desktop.
- Provide a flexible application delivery solution. If users have local applications that you cannot virtualize or that IT does not maintain, those applications still behave as though they are installed on a virtual desktop.
- Eliminate double-hop latency when applications are hosted separately from the virtual desktop, by putting a shortcut to the published application on the user's Windows device.
- Use applications such as:
  - Video conferencing software such as GoToMeeting.
  - Specialty or niche applications that are not yet virtualized.
  - Applications and peripherals that would otherwise transfer large amounts of data from a user device to a server and back to the user device, such as DVD burners and TV tuners.

In XenApp and XenDesktop, hosted desktop sessions use URL redirection to launch Local App Access applications. URL redirection makes the application available under more than one URL address. It launches a local browser (based on the browser's URL blacklist) by selecting embedded links within a browser in a desktop session. If you navigate to a URL that is not present in the blacklist, the URL is opened in the desktop session again.

URL redirection works only for desktop sessions, not application sessions. The only redirection feature you can use for application sessions is host-to-client content redirection, which is a type of server FTA. This FTA redirects certain protocols to the client, such as http, https, rtsp, or mms. For example, if you only open embedded links with http, the links directly open with the client application. There is no URL blacklist or whitelist support.

When Local App Access is enabled, URLs that are displayed to users as links from locally-running applications, from user-hosted applications, or as shortcuts on the desktop are redirected in one of the following ways:

- From the user's computer to the hosted desktop
- From the XenApp or XenDesktop server to the user's computer
- Rendered in the environment in which they are launched (not redirected)

To specify the redirection path of content from specific Web sites, configure the URL whitelist and URL blacklist on the Virtual Delivery Agent. Those lists contain multi-string registry keys that specify the URL redirection policy settings; for more information, see the Local App Access policy settings.

URLs can be rendered on the VDA with the following exceptions:

- Geo/Locale information — Web sites that require locale information, such as msn.com or news.google.com (opens a country specific page based on the Geo). For example, if the VDA is provisioned from a data center in the UK and the client is connecting from India, the user expects to see in.msn.com but instead sees uk.msn.com.
- Multimedia content — Web sites containing rich media content, when rendered on the client device, give the end users a native experience and also save bandwidth even in high latency networks. Although there is Flash redirection feature, this complements by redirecting sites with other media types such as Silverlight. This is in a very secure environment. That is, the URLs that are approved by the administrator are run on the client while the rest of the URLs are redirected to the VDA.

In addition to URL redirection, you can use File Type Association (FTA) redirection. FTA launches local applications when a file is encountered in the session. If the local app is launched, it must have access to the file to open it. Therefore, you can

only open files that reside on network shares or on client drives (using client drive mapping) using local applications. For example, when opening a PDF file, if a PDF reader is a local app, then the file opens using that PDF reader. Because the local app can access the file directly, there is no network transfer of the file through ICA to open the file.

Local App Access is supported on the valid operating systems for VDAs for Windows Server OS and VDAs for Windows Desktop OS, and requires Citrix Receiver for Windows version 4.1 (minimum). The following browsers are supported:

- Internet Explorer 8, 9, 10, and 11
- Firefox 3.5 through 21.0
- Chrome 10

Review the following considerations and limitations when using Local App Access and URL redirection.

- Local App Access is designed for full-screen, virtual desktops spanning all monitors:
  - The user experience can be confusing if Local App Access is used with a virtual desktop that runs in windowed mode or does not cover all monitors.
  - For multiple monitors, when one monitor is maximized it becomes the default desktop for all applications launched in that session, even if subsequent applications typically launch on another monitor.
  - The feature supports one VDA; there is no integration with multiple concurrent VDAs.
- Some applications can behave unexpectedly, affecting users:
  - Users might be confused with drive letters, such as local C: rather than virtual desktop C: drive.
  - Available printers in the virtual desktop are not available to local applications.
  - Applications that require elevated permissions cannot be launched as client-hosted applications.
  - There is no special handling for single-instance applications (such as Windows Media Player).
  - Local applications appear with the Windows theme of the local machine.
  - Full-screen applications are not supported. This includes applications that open to full screen, such as PowerPoint slide shows or photo viewers that cover the entire desktop.
  - Local App Access copies the properties of the local application (such as the shortcuts on the client's desktop and Start menu) on the VDA; however, it does not copy other properties such as shortcut keys and read-only attributes.
  - Applications that customize how overlapping window order is handled can have unpredictable results. For example, some windows might be hidden.
  - Shortcuts are not supported, including My Computer, Recycle Bin, Control Panel, Network Drive shortcuts, and folder shortcuts.
  - The following file types and files are not supported: custom file types, files with no associated programs, zip files, and hidden files.
  - Taskbar grouping is not supported for mixed 32-bit and 64-bit client-hosted or VDA applications, such as grouping 32-bit local applications with 64-bit VDA applications.
  - Applications cannot be launched using COM. For example, if you click an embedded Office document from within an Office application, the process launch cannot be detected, and the local application integration fails.
- URL redirection supports only explicit URLs (that is, those appearing in the browser's address bar or found using the in-browser navigation, depending on the browser).
- URL redirection works only with desktop sessions, not with application sessions.
- The local desktop folder in a VDA session does not allow users to create new files.
- Multiple instances of a locally-running application behave according to the taskbar settings established for the virtual desktop. However, shortcuts to locally-running applications are not grouped with running instances of those applications. They are also not grouped with running instances of hosted applications or pinned shortcuts to hosted applications. Users can close only windows of locally-running applications from the Taskbar. Although users can pin local application windows to the desktop Taskbar and Start menu, the applications might not launch consistently when using

these shortcuts.

The Local App Access interaction with Windows includes the following behaviors.

- Windows 8 and Windows Server 2012 short cut behavior
  - Windows Store applications installed on the client are not enumerated as part of Local App Access shortcuts.
  - Image and video files are usually opened by default using Windows store applications. However, Local App Access enumerates the Windows store applications and opens shortcuts with desktop applications.
- Local Programs
  - For Windows 7, the folder is available in the Start menu.
  - For Windows 8, Local Programs is available only when the user chooses All Apps as a category from the Start screen. Not all subfolders are displayed in Local Programs.
- Windows 8 graphics features for applications
  - Desktop applications are restricted to the desktop area and are covered by the Start screen and Windows 8 style applications.
  - Local App Access applications do not behave like desktop applications in multi-monitor mode. In multi-monitor mode, the Start screen and the desktop display on different monitors.
- Windows 8 and Local App Access URL Redirection
  - Because Windows 8 Internet Explorer has no add-ons enabled, use desktop Internet Explorer to enable URL redirection.
  - In Windows Server 2012, Internet Explorer disables add-ons by default. To implement URL Redirection, disable Internet Explorer enhanced configuration. Then reset the Internet Explorer options and restart to ensure that add-ons are enabled for standard users.

Configure Local App Access and URL redirection

Sep 18, 2015

To use Local App Access and URL redirection with Citrix Receiver:

- Install Receiver on the local client machine. You can enable both features during Receiver installation or you can enable Local App Access template using the Group Policy editor.
- Set the Allow local app access policy setting to Enabled. You can also configure URL whitelist and blacklist policy settings for URL redirection. For more information, see Local App Access policy settings.

To enable Local App Access and URL redirection for all local applications:

1. Set the Allow local app access policy setting to Enabled. When this setting is enabled, the VDA allows the client to decide whether administrator-published applications and Local App Access shortcuts are enabled in the session. (When this setting is disabled, both administrator-published applications and Local App Access shortcuts do not work for the VDA.) This policy setting applies to the entire machine, as well as the URL redirection policy.
2. Enable Local App Access and URL redirection when you install Citrix Receiver for all users on a machine. This action also registers the browser add-ons required for URL redirection.
   From the command prompt, run the appropriate command to install the Receiver with the following option:
   `CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1`
   `CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1`

1. Run gpedit.msc.
2. Select Computer Configuration. Right-click Administrative Templates and select Add/Remote Templates > Add.
3. Add the icaclient.adm template located in the Receiver Configuration folder (usually in c:\Program Files (x86)\Citrix\Online Plugin\Configuration). (After the icaclient.adm template is added to Computer Configuration, it is also available in User Configuration.)
4. Expand Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User Experience.
5. Select Local App Access settings.
6. Select Enabled and then select Allow URL Redirection. For URL redirection, register browser add-ons using the command line, as described below.

To provide access to only published applications:

1. On the server where the Delivery Controller is installed, run regedit.exe.
   1. Navigate to HKLM\Software\Wow6432Node\Citrix\DesktopStudio.
   2. Add the REG_DWORD entry ClientHostedAppsEnabled with a value of 1. (A 0 value disables Local App Access.)
2. Restart the Delivery Controller server and then restart Studio.
3. Publish Local App Access applications.
   1. Select Delivery Groups in the Studio navigation pane and then select the Applications tab.
   2. Select Create Local Access Application in the Actions pane.
   3. Select the desktop Delivery Group.
   4. Enter the full executable path of the application on the user's local machine.
   5. Indicate if the shortcut to the local application on the virtual desktop will be visible on the Start menu, the desktop, or

both.

6. Accept the default values on the Name page and then review the settings.

4. Enable Local App Access and URL redirection when you install Citrix Receiver for all users on a machine. This action also registers the browser add-ons required for URL redirection.
   From the command prompt, run the command to install the Receiver with the following option:
   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
5. Set the Allow local app access policy setting to Enabled. When this setting is enabled, the VDA allows the client to decide whether administrator-published applications and Local App Access shortcuts are enabled in the session. (When this setting is disabled, both administrator-published applications and Local App Access shortcuts do not work for the VDA.)

Note: The browser add-ons required for URL redirection are registered automatically when you install Receiver from the command line with the /ALLOW_CLIENTHOSTEDAPPSURL=1 option.
You can use the following commands to register and unregister one or all add-ons:

- To register add-ons on a client device: <client-installation-folder>\redirector.exe /reg<browser>
- To unregister add-ons on a client device: <client-installation-folder>\redirector.exe /unreg<browser>
- To register add-ons on a VDA: <VDAinstallation-folder>\VDARedirector.exe /reg<browser>
- To unregister add-ons on a VDA: <VDAinstallation-folder>\VDARedirector.exe /unreg<browser>

where <browser> is IE, FF, Chrome, or All.

For example, the following command registers Internet Explorer add-ons on a device running Receiver.
C:\Program Files\Citrix\ICA Client\redirector.exe/regIE
The following command registers all add-ons on a Windows Server OS VDA.
C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regAll

Description	Configuration
By default, Internet Explorer redirects the URL entered. If the URL is not in the blacklist but is redirected to another URL by the browser or website, the final URL is not redirected, even if it is on the blacklist.	For URL redirection to work correctly, enable the add-on when prompted by the browser. If the add-ons using Internet options or the add-ons in the prompt are disabled, URL redirection does not work correctly.
The Firefox add-ons always redirect the URLs.	When an add-on is installed, Firefox prompts to allow/prevent installing the add-on on a new tab page. You must allow the add-on for the feature to work.
The Chrome add-on always redirects the final URL that is navigated and not the entered URLs.	The extensions have been installed externally. If you disable the extension, the URL redirection feature does not work in Chrome. If the URL redirection is required in Incognito mode, allow the extension to run in that mode in the browser Settings.

1. On the hosted desktop, run gpedit.msc.
    1. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State.
    For a 64-bit system, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State.
    2. Add the REG_DWORD entry Terminate with one of the values:
        - 1 - Local applications continue to run when a user logs off or disconnects from the virtual desktop. Upon reconnection, local applications are reintegrated if they are available in the local environment.
        - 3 - Local applications close when a user logs off or disconnects from the virtual desktop.

Server VDI

Oct 24, 2016

Use the Server VDI (Virtual Desktop Infrastructure) feature to deliver a desktop from a server operating system for a single user.

- Enterprise administrators can deliver server operating systems as VDI desktops, which can be valuable for users such as engineers and designers.
- Service Providers can offer desktops from the cloud; those desktops comply with the Microsoft Services Provider License Agreement (SPLA).

You can use the Enhanced Desktop Experience Citrix policy setting to make the server operating system look like a Windows 7 operating system.

The following features cannot be used with Server VDI:

- Personal vDisks
- HDX 3D Pro
- Hosted applications
- Local App Access
- Direct (non-brokered) desktop connections
- Remote PC Access

For Server VDI to work with TWAIN devices such as scanners, the Windows Server Desktop Experience feature must be installed. In Windows Server 2012, this is an optional feature which you install from Administrative Tools > Server Manager > Features > Add features > Desktop Experience.

Server VDI is supported on the same server operating systems as the VDA for Windows Server OS.

1. Prepare the Windows server for installation: ensure that Remote Desktop Services role services are not installed and that users are restricted to a single session:
   - Use Windows Server Manager to ensure that the Remote Desktop Services role services are not installed. If they were previously installed, remove them.
   - Ensure that the 'Restrict each user to a single session' property is enabled.
     - On Windows Server 2008 R2, access this property through Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration. In the Edit settings > General section, the Restrict each user to a single session setting should indicate Yes.
     - On Windows Server 2012, edit the registry to set the Terminal Server setting. In registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer to set DWORD fSingleSessionPerUser to 1.
2. For Windows Server 2008 R2, install Microsoft .NET Framework 3.5 SP1 on the server before installing the VDA.
3. Use the command line interface to install a VDA on a supported server or server master image, specifying the /quiet and /servervdi options. (By default, the installer blocks the Windows Desktop OS VDA on a server operating system; using the command line overrides this behavior.)
   XenDesktopVdaSetup.exe /quiet /servervdi

   You can specify the Delivery Controller or Controllers while installing the VDA using the command line, using the **/controllers** option.

   Use the **/enable_hdx_ports** option to open porst in the firewall, unless the firewall is to be configured manually.

   Add the **/masterimage** option if you are installing the VDA on an image, and will use MCS to create server VMs from that image.

   Do not include options for features that are not supported with Server VDI, such as /baseimage, /enable_hdx_3d_pro, or /xa_server_location.

4. Create a Machine Catalog for Server VDI.
   1. On the Operating System page, select Windows Desktop OS.
   2. On the Summary page, specify a machine catalog name and description for administrators that clearly identifies it as Server VDI; this will

be the only indicator in Studio that the catalog supports Server VDI.

When using Search in Studio, the Server VDI catalog you created is displayed on the Desktop OS Machines tab, even though the VDA was installed on a server.

5. Create a Delivery Group and assign the Server VDI catalog you created in the previous step.

If you did not specify the Delivery Controllers while installing the VDA, specify them afterward using Citrix policy setting, Active Directory, or by editing the VDA machine's registry values.

Remove components

Sep 09, 2015

To remove components, Citrix recommends using the Windows feature for removing or changing programs. Alternatively, you can remove components using the command line, or a script on the installation media.

When you remove components, prerequisites are not removed, and firewall settings are not changed. When you remove a Controller, the SQL Server software and the databases are not removed.

Before removing a Controller, remove it from the Site. Before removing Studio or Director, Citrix recommends closing them.

If you upgraded a Controller from an earlier deployment that included Web Interface, you must remove the Web Interface component separately; you cannot use the installer to remove Web Interface.

To remove components using the Windows feature for removing or changing programs

From the Windows feature for removing or changing programs:

- To remove a Controller, Studio, Director, License Server, or StoreFront, select Citrix XenApp <version> or Citrix XenDesktop <version>, then right-click and select Uninstall. The installer launches, and you can select the components to be removed.
  Alternatively, you can remove StoreFront by right-clicking Citrix StoreFront and selecting Uninstall.
- To remove a VDA, select Citrix Virtual Delivery Agent <version>, then right-click and select Uninstall. The installer launches and you can select the components to be removed.
- To remove the Universal Print Server, select Citrix Universal Print Server, then right-click and select Uninstall.

To remove core components using the command line

From the \x64\XenDesktop Setup directory on the installation media, run the XenDesktopServerSetup.exe command.

- To remove one or more components, use the /remove and /components options.
- To remove all components, use the /removeall option.

For command and parameter details, see Install using the command line.

For example, the following command removes Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

To remove a VDA using the command line

From the \x64\XenDesktop Setup directory on the installation media, run the XenDesktopVdaSetup.exe command.

- To remove one or more components, use the /remove and /components options.
- To remove all components, use the /removeall option.

For command and parameter details, see Install using the command line.

For example, the following command removes the VDA and Receiver.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

To remove VDAs using a script in Active Directory; see Install or remove Virtual Delivery Agents using scripts.

Upgrades and migration

Sep 19, 2014

Upgrade

Upgrading changes deployments to the newest component versions without having to set up new machines or Sites; this is known as an in-place upgrade. You can upgrade:

- From XenDesktop version 5 (or a later version) to XenDesktop 7.6
- From XenApp version 7.5 to XenApp 7.6

You can also upgrade a XenApp 6.5 worker server to a XenApp 7.6 VDA for Windows Server OS. This is a supplementary activity to migrating XenApp 6.5.

To upgrade a XenDesktop 5 (or later) farm or a XenApp 7.5 Site:

1. Run the installer on the machines where the core components and VDAs are installed. The software determines if an upgrade is available and installs the newer version.
2. Use the newly upgraded Studio to upgrade the database and the Site.

For more information, see Upgrade a deployment.

For information about installing Controller hotfixes, see Knowledge Center article CTX201988.

To upgrade a XenApp 6.5 worker server to a XenApp 7.6 VDA:

1. Run the product installer on the XenApp 6.5 worker server. The software removes the server from the XenApp 6.5 farm, removes the XenApp 6.5 software, and installs a 7.6 VDA for Windows Server OS.
2. After upgrading the server, add it to machine catalogs and Delivery Groups in the 7.6 Site.

For more information, see Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS.

Migrate

Migrating moves data from an earlier deployment to the newest version. You can migrate a XenApp 6.5 or a XenDesk 4 deployment. Migrating includes installing 7.6 components and creating a new Site, exporting data from the older farm, and then importing the data to the new Site.

To migrate from XenApp 6.5:

1. Install core components and create a new XenApp Site.
2. From the XenApp 6.5 controller, use PowerShell cmdlets to export policy and/or farm data to XML files. You can edit the XML file content to tailor the information you will import.
3. From the new 7.6 Site, use PowerShell cmdlets and the XML files to import policy and/or application data to the new Site.
4. Complete post-migration tasks on the new Site.

For more information, see Migrate XenApp 6.x.

To migrate from XenDesktop 4:

1. Install core components and create a new XenDesktop Site.
2. From the XenDesktop 4 farm, use the export command tool to export farm data to an XML file. You can edit the XML file content to tailor the information you will import.
3. From the 7.6 Site, use the import command tool and the XML file to import the farm data to the new Site.

4. Complete post-migration tasks on the new Site.

For more information, see Migrate XenDesktop 4.

Upgrade a deployment

Aug 15, 2016

You can upgrade certain deployments to newer versions without having to first set up new machines or Sites; this is called an in-place upgrade. You can upgrade:

- From XenDesktop version 5 (or a later version) to the latest released (current) XenDesktop version
- From XenApp version 7.5 (or a later version) to the latest released (current) XenApp version

You can also use the XenApp 7.6 installer to upgrade a XenApp 6.5 worker server to a XenApp 7.6 VDA for Windows Server OS. This is a supplementary activity to migrating XenApp 6.5; see Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS.

To start an upgrade, you run the installer from the new version to upgrade previously installed core components (Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server) and VDAs. The installer determines which components require upgrading and then starts the upgrade at your command. After upgrading the components, you use the newly upgraded Studio to upgrade the Site database and the Site.

In this content, the word product refers to XenApp 7.x or XenDesktop 7.x, unless otherwise noted.

You cannot upgrade:

- From an Early Release or Technology Preview version
- From a XenApp version earlier than 7.5 (except replacing XenApp 6.5 software on a server with a current VDA for Server OS; see Migrate XenApp 6.x)
- From a XenDesktop version earlier than 5.6; see Migrate XenDesktop 4
- From XenApp to XenDesktop, or from XenDesktop to XenApp

Which product component versions can be upgraded?

Using the product installer and Studio, you can upgrade:

- Delivery Controllers 5 or later
- VDA 5.0 SP1 or later
  - Unlike earlier VDA releases, you must use the product installer to upgrade VDAs; you cannot use MSIs.
  - If the installer detects Receiver for Windows (Receiver.exe) on the machine, it is upgraded to the Receiver version included on the product installation media.
  - If the installer detects Receiver for Windows Enterprise (CitrixReceiverEnterprise.exe) on the machine, it is upgraded to Receiver for Windows Enterprise 3.4.
- Director 1 or later
- Database - This upgrades the schema and migrates data for the Site database (plus the Configuration Logging and Monitoring databases, if you're upgrading from an earlier 7.x version)
- Personal vDisk

Using the guidance in the feature/product documentation, upgrade the following if needed:

- Provisioning Services (for XenApp 7.x and XenDesktop 7.x, Citrix recommends using the latest released version; the minimum supported version is Provisioning Services 7.0).
  - Upgrade the Provisioning Services server using the server rolling upgrade, and the clients using vDisk versioning.
  - Provisioning Services 7.x does not support creating new desktops with XenDesktop 5 versions. So, although existing desktops will continue to work, you cannot use Provisioning Services 7.x to create new desktops until you upgrade XenDesktop. Therefore, if you plan a mixed environment of XenDesktop 5.6 and 7.x Sites, do not upgrade Provisioning Services to version 7.
- Microsoft System Center Virtual Machine Manager SCVMM. The current product supports SCVMM 2012 and SCVMM 2012 SP1; XenDesktop 5.x supports earlier versions. Use the following upgrade sequence to avoid downtime:

1. If you have Controllers running versions earlier than XenDesktop 5.6 FP1, upgrade them to XenDesktop 5.6 FP1 (see the XenDesktop documentation for that version).
2. Upgrade the SCVMM server to SCVMM 2012; see the Microsoft documentation for instructions.
3. Upgrade XenDesktop components to the current version.
4. Optionally, upgrade the SCVMM server to SCVMM 2012 SP1.

- StoreFront.

Requirements, limits, and preparation

	You must use the product installer's graphical or command-line interface to upgrade core components and VDAs; you cannot import or migrate data from an earlier version.
	If you install or upgrade any components to the new version but choose not to upgrade other components (on different machines) that require upgrade, Studio will remind you. For example, if an upgrade includes new versions of the Controller and Studio, and you upgrade only the Controller (but you do not run the installer on the machine where Studio is installed), Studio will not let you continue to manage the Site until you upgrade Studio.
	Before upgrading the Citrix License Server, be sure your Subscription Advantage date is valid for the new product version. If you are upgrading from an earlier 7.x product version, the date must be at least 2013.0522.
	You cannot upgrade XenDesktop Express Edition. Obtain and install a license for a currently supported edition, then upgrade it.
	Before beginning any upgrade activity, back up the database, as described in CTX135207, so you can restore it if any issues are discovered after the database upgrade.
	Optionally, back up templates and upgrade hypervisors, if used.
	If you must continue to run earlier version Sites and current version Sites, see Mixed environment considerations.
	If you have VDAs installed on Windows XP or Windows Vista machines, see VDAs on machines running Windows XP or Windows Vista.
	If you do not plan to upgrade all VDAs to the latest version, review Mixed VDA support.
	If your deployment includes Web Interface, Citrix recommends using StoreFront.
	In addition to being a domain user, you must be a local administrator on the machines where you are upgrading product components.

•	When you upgrade, you do not choose or specify the product (XenApp or XenDesktop), which was set during the initial installation.
	Review the upgrade sequence below so you can plan for and mitigate potential outages.

Mixed environment considerations

When your environment contains Sites/farms with different product versions (a mixed environment), Citrix recommends using StoreFront to aggregate applications and desktops from different product versions (for example, if you have a XenDesktop 7.1 Site and a XenDesktop 7.5 Site). For details, see the StoreFront documentation.

- Generally, the current Studio and Director versions manage/monitor only current Sites. (Although this version of Director can monitor XenDesktop 5.x VDAs, some data (including logon duration) will not be available for those VDAs.) For example, you cannot manage a XenDesktop 7.1 Site with Studio version 7.6. Similarly, you cannot manage a XenDesktop 7.6 Site with a Studio version 7.1.
- You can use current VDAs in deployments containing earlier Controller versions. Keep in mind that in such cases, new features in the current release may not be available. See
  — Mixed VDA considerations
  below.
- Sites with Controllers at version 5.x and VDAs at version 7.x should remain in that state only temporarily. Ideally, you should complete the upgrade of all components as soon as possible.
- In a mixed environment, continue using the Studio and Director versions for each release, but make sure that different versions are installed on separate machines.
- If you plan to run XenDesktop 5.6 and 7.x Sites simultaneously and use Provisioning Services for both, either deploy a new Provisioning Services for use with the 7.x Site, or upgrade the current Provisioning Services and be unable to provision new workloads in the XenDesktop 5.6 Site.
- Do not upgrade a standalone Studio version until you are ready to use the new version.

VDAs on machines running Windows XP or Windows Vista

You cannot upgrade VDAs installed on machines running Windows XP or Windows Vista to a 7.x version. You must use VDA 5.6 FP1 with certain hotfixes; see CTX140941 for instructions. Although earlier-version VDAs will run in a 7.x Site, they cannot use many of its features, including:

- Features noted in Studio that require a newer VDA version.
- Configuring App-V applications from Studio.
- Configuring Receiver StoreFront addresses from Studio.
- Automatic support for Microsoft Windows KMS licensing when using Machine Creation Services. See CTX128580.
- Information in Director:
  - Logon times and logon end events impacting the logon duration times in the Dashboard, Trends, and User Detail views.
  - Logon duration breakdown details for HDX connection and authentication time, plus duration details for profile load, GPO load, logon script, and interactive session establishment.
  - Several categories of machine and connection failure rates.
  - Activity Manager in the Help Desk and User Details views.

Citrix recommends reimaging Windows XP and Windows Vista machines to a supported operating system version and then installing the latest VDA.

VDAs on machines running Windows 8.x and Windows 7

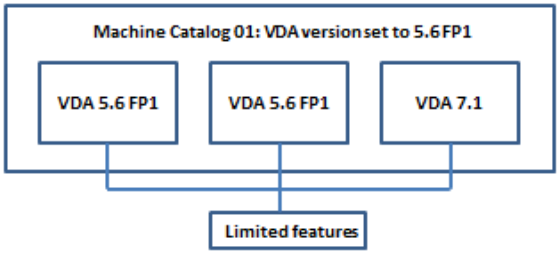
To upgrade VDAs installed on machines running Windows 8.x or Window 7 to Windows 10, Citrix recommends reimaging Windows 7 and Windows 8.x machines to Windows 10 and then installing the supported VDA for Windows 10, using the standalone VDA installation package delivered with XenApp and XenDesktop 7.6 FP3. If reimaging is not an option, uninstall the VDA prior to upgrading the operating system, otherwise the VDA will be in an unsupported state.

Mixed VDA support

When you upgrade the product to a later version, Citrix recommends you upgrade all the core components and VDAs so you can access all the new and enhanced features in your edition. For example, to use the session prelaunch, session linger, and unauthenticated users features in the 7.6 release, the VDAs must have a minimum version of 7.6 installed.

In some environments, you may not be able to upgrade all VDAs to the most current version. In this scenario, when you create a machine catalog, you can specify the VDA version installed on the machines. By default, this setting specifies the latest recommended VDA version; you need to consider changing this setting only if the machine catalog contains machines with earlier VDA versions. However, mixing VDA versions in a machine catalog can have unintended effects

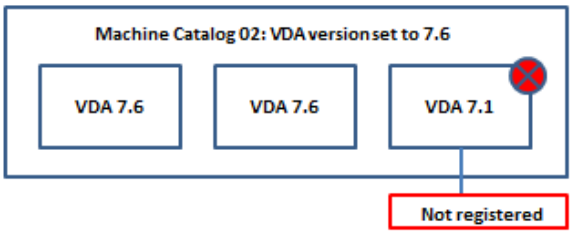
As noted above, if your deployment includes Windows XP and Windows Vista systems, you must use an earlier VDA version, and the machine catalog containing those machines must specify VDA version 5.6 FP1. The VDAs will register successfully with the Controller, but those machines will be unable to use many of the new features in the 7.x versions (including StoreFront). This also applies to any machines you add to that catalog that have 7.x version VDAs. The following graphic illustrates this.



In the above case, if you must continue to use older VDAs, place them in a machine catalog by themselves.

If a machine catalog is created with the default recommended VDA version setting, and any of the machines in the catalog has an earlier VDA version installed, those machines will not be able to register with the Controller and will not work.

For example, assume the most recent VDA version is 7.6. You create a machine catalog with the default VDA setting: "7.6 (recommended, to access the latest features)." You add three machines to that catalog: two with VDA 7.6 and one with VDA 7.1.

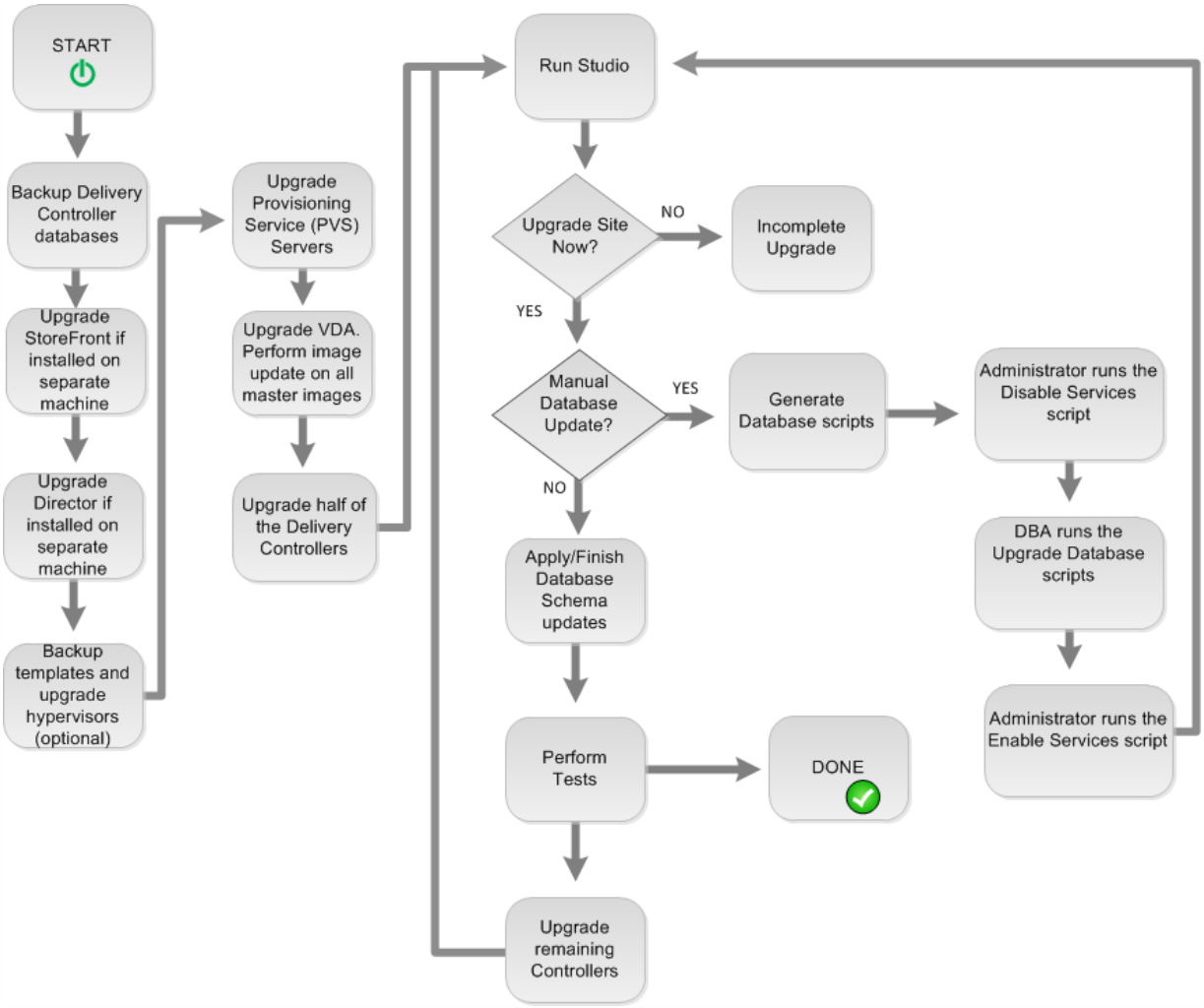


In this example, the machine with VDA 7.1 will not register with the Controller. If you cannot upgrade that VDA, consider creating a separate machine catalog configured with a VDA setting of "version 7.0 or later" and adding that machine. Although that machine will not be able to take advantage of new 7.6 features, it will be able to register with the Controller.

Upgrade sequence

If components are installed on different machines, you run the installer on each of those machines.

The upgrade sequence is illustrated below; descriptions follow.



To run the product installer graphical interface, log on to the machine and then insert the media or mount the ISO drive for the new release. Double-click AutoSelect. To use the command-line interface, see

— Install using the command line

.

1. If more than one core component is installed on the same server (for example, the Controller, Studio, and License Server) and several of those components have new versions available, they will all be upgraded when you run the installer on that server. If any core components are installed on machines other than the Controller, run the installer on each of those machines (in the preferred order: License Server, StoreFront, and then Director).
2. Upgrade the Provisioning Services servers and clients, using the guidance in the Provisioning Services documentation.
3. Run the product installer on machines containing VDAs. Although you can upgrade VDAs before or after upgrading the Controllers, Citrix recommends you do so before, because it allows you to quickly enable new features after the upgrade. When upgrading VDAs from an earlier 7.x version that are installed on physical machines (including Remote PC Access), use the command-line interface with the parameter: /EXCLUDE "Personal vDisk","Machine Identity Service". For example:
   C:\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /EXCLUDE "Personal vDisk","Machine Identity Service"
4. Run the product installer on half of the Controllers. (This will also upgrade any other core components installed on those servers.) For example, if your Site has four Controllers, run the installer on two of them.
   - Leaving half of the Controllers active allows users to access the Site. VDAs can register with the remaining Controllers. There may be times when the Site has reduced capacity because fewer Controllers are available. The upgrade causes only a brief interruption in establishing new client connections during the final database upgrade steps. The upgraded Controllers cannot process requests until the entire Site is upgraded.
   - If your Site has only one Controller, the Site is inoperable during the upgrade.
5. If Studio is installed on a different machine than one of the Controllers you upgraded in the previous step, run the installer on

the machine where Studio is installed.

6. From the newly upgraded Studio, upgrade the Site database. For details, see Upgrade the database and Site.
7. From the newly upgraded Studio, select Citrix Studio site-name in the navigation pane. Select the Common Tasks tab. Select Upgrade remaining Delivery Controllers.
8. After completing the upgrade and confirming completion, close and then reopen Studio.
9. In the Site Configuration section of the Common Tasks page, select Perform registration. Registering the Controllers makes them available to the Site.
10. After you select Finish when the upgrade completes, you are offered the opportunity to enroll in the Citrix Customer Experience Improvement Program (CEIP), which collects anonymous information about your deployment. That information is then used to improve product quality, reliability, and performance.
11. After upgrading components, the database, and the Site, use Studio to:
    - Test the newly-upgraded Site. From Studio, select Citrix Studio site-name in the navigation pane. Select the Common Tasks tab and then select Test Site. These tests were run automatically after you upgraded the database, but you can run them again at any time.
    - Update all master images that use the upgraded VDA.
    - Upgrade machine catalogs and Delivery Groups.

Upgrade the database and Site

After upgrading the core components and VDAs, use the newly upgraded Studio to initiate an automatic or manual database and Site upgrade.

- For an automatic database upgrade, the Studio user's permissions must include the ability to update the SQL Server database schema (for example, the db_securityadmin or db_owner database role).
- If the Studio user does not have those permissions, initiating a manual database upgrade will generate scripts. The Studio user runs some of the scripts from Studio; the database administrator runs other scripts using a tool such as SQL Server Management Studio. If the SQL scripts are run manually, they should be run using either the SQLCMD utility or using the SQL Management Studio in SQLCMD mode. Inaccurate errors may result otherwise.

Important: Citrix strongly recommends you back up the database before upgrading, as described in CTX135207.
During a database upgrade, product services are disabled. During that time, Controllers cannot broker new connections for the Site, so plan carefully.

After the database upgrade completes and product services are enabled, Studio tests the environment and configuration, and then generates an HTML report. If problems are identified, you can restore the database backup. After resolving issues, you can upgrade the database again.

Upgrade the database and Site automatically - Launch the newly upgraded Studio. After you choose to start the Site upgrade automatically and confirm that you are ready, the database and Site upgrade proceeds.

Upgrade the database and Site manually - This process includes generating and running scripts.

1. Launch the newly upgraded Studio. After you choose to manually upgrade the Site, the wizard checks for License Server compatibility and requests confirmation. After you confirm that you have backed up the database, the wizard generates and displays the scripts and a checklist of upgrade steps.
2. Run the following scripts in the order shown:

Script	Description
DisableServices.ps1	PowerShell script to be run by the Studio user on a Controller to disable product services.

Script	Description
UpgradeSiteDatabase.sql	SQL script to be run by the database administrator on the server containing the Site database, using a tool such as SQL Server Management Studio.
UpgradeMonitorDatabase.sql	SQL script to be run by the database administrator on the server containing the Monitor database, using a tool such as SQL Server Management Studio.
UpgradeLoggingDatabase.sql	SQL script to be run by the database administrator on the server containing the Configuration Logging database, using a tool such as SQL Server Management Studio. Run this script only if this database changes (for example, after applying a hotfix).
EnableServices.ps1	PowerShell script to be run by the Studio user on a Controller to enable product services.

3. After you complete the displayed checklist tasks, select Finish upgrade.

Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS

Aug 25, 2014

When you run the XenApp 7.6 installer on a XenApp 6.5 worker server, it:

- Removes the server from the XenApp 6.5 farm (this task automatically invokes the XenApp 6.5 installer's command-line interface)
- Removes the XenApp 6.5 software
- Installs a new (XenApp 7.6 or later supported release) VDA for Windows Server OS

When you use the installer's graphical interface, you are guided through the same wizard that you used when installing VDAs for Windows Server OS in your new XenApp Site. Similarly, the command-line interface uses the same commands and parameters you use to install other VDAs.

You are probably already familiar with using the installer from installing your XenApp 7.6 core components and other VDAs. To review preparatory information, see VDA installation preparation. Then, launch the installer (Install using the graphical interface) or issue the command (Install a VDA using the command line) on the XenApp 6.5 worker server.

Good to know:

- This upgrade is valid on XenApp 6.5 servers that are configured in session-host only mode (also called session-only or worker servers).
- Uninstalling XenApp 6.5 requires several server restarts. When using the command-line interface, you can use the /NOREBOOT option to inhibit that automatic action; however, you must restart the server for the uninstallation and subsequent installation to proceed.
- If an error occurs during the XenApp uninstallation process, check the uninstall error log referenced in the error message. Uninstall log files reside in the folder "%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\."
- After you upgrade the XenApp 6.5 worker servers, from Studio in the new XenApp Site, create Machine Catalogs (or edit existing catalogs) for the upgraded workers.
- If you migrated policy and application settings from a XenApp 6.5 controller server (see Migrate XenApp 6.x), assign the Delivery Groups containing the migrated published applications to the machine catalog that hosted those applications in XenApp 6.5.

Troubleshooting

Symptoms: Removal of the XenApp 6.5 software fails. The uninstall log contains the message: "Error 25703. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Scripts directory. Please make sure that your IIS installation is correct."

- Cause: The issue occurs on systems where (1) during the initial XenApp 6.5 installation, you indicated that the Citrix XML Service (CtxHttp.exe) should not share a port with IIS, and (2) .NET Framework 3.5.1 is installed.
- Resolution:
  1. Remove the Web Server (IIS) role using the Windows Remove Server Roles wizard. (You can reinstall the Web Server (IIS) role later.)
  2. Restart the server.
  3. Using Add/Remove Programs, uninstall the following:
     1. Citrix XenApp 6.5
     2. Microsoft Visual C++ 2005 Redistributable (x64), version 8.0.56336

4. Restart the server.
5. Run the XenApp 7.6 installer to install the VDA for Windows Server OS.

Migrate XenApp 6.x

Sep 01, 2015

Important: Review this entire article before beginning a migration.

The XenApp 6.x Migration Tool (the migration tool) is a collection of PowerShell scripts containing cmdlets that migrate XenApp 6.x (6.0 or 6.5) policy and farm data. On the XenApp 6.x controller server, you run export cmdlets that gather that data into XML files. Then, from the XenApp 7.6 Controller, you run import cmdlets that create objects using the data gathered during the export.

A video overview of the migration tool is available here.

The following sequence summarizes the migration process; details are provided later.

1. On a XenApp 6.0 or 6.5 controller:
   1. Import the PowerShell export modules.
   2. Run the export cmdlets to export policy and/or farm data to XML files.
2. Copy the XML files (and icons folder if you chose not to embed them in the XML files during the export) to the XenApp 7.6 Controller.
3. On the XenApp 7.6 Controller:
   1. Import the PowerShell import modules.
   2. Run the import cmdlets to import policy and/or farm data (applications), using the XML files as input.
4. Complete post-migration steps.

Before you run an actual migration, you can export your XenApp 6.x settings and then perform a preview import on the XenApp 7.6 site. The preview identifies possible failure points so you can resolve issues before running the actual import. For example, a preview might detect that an application with the same name already exists in the new XenApp 7.6 site. You can also use the log files generated from the preview as a migration guide.

Unless otherwise noted, the term 6.x refers to XenApp 6.0 or 6.5.

New in this release

This December 2014 release (version 20141125) contains the following updates:

- If you encounter issues using the migration tool on a XenApp 6.x farm, report them to the support forum http://discussions.citrix.com/forum/1411-xenapp-7x/, so that Citrix can investigate them for potential improvements to the tool.
- New packaging - the XAMigration.zip file now contains two separate, independent packages: ReadIMA.zip and ImportFMA.zip. To export from a XenApp 6.x server, you need only ReadIMA.zip. To import to a XenApp 7.6 server, you

need only ImportFMA.zip.

- The Export-XAFarm cmdlet supports a new parameter (EmbedIconData) that eliminates the need to copy icon data to separate files.
- The Import-XAFarm cmdlet supports three new parameters:
  - MatchServer - import applications from servers whose names match an expression
  - NotMatchServer - import applications from servers whose names do not match an expression
  - IncludeDisabledApps - import disabled applications
- Prelaunched applications are not imported.
- The Export-Policy cmdlet works on XenDesktop 7.x.

Migration Tool package

The migration tool is available under the XenApp 7.6 Citrix download site. The XAMigration.zip file contains two separate, independent packages:

- ReadIMA.zip - contains the files used to export data from your XenApp 6.x farm, plus shared modules.

Module or file	Description
ExportPolicy.psm1	PowerShell script module for exporting XenApp 6.x policies to an XML file.
ExportXAFarm.psm1	PowerShell script module for exporting XenApp 6.x farm settings to an XML file.
ExportPolicy.psd1	PowerShell manifest file for script module ExportPolicy.psm1.
ExportXAFarm.psd1	PowerShell manifest file for script module ExportXAFarm.psm1.
LogUtilities.psm1	Shared PowerShell script module that contains logging functions.
XmlUtilities.psd1	PowerShell manifest file for script module XmlUtilities.psm1.
XmlUtilities.psm1	Shared PowerShell script module that contains XML functions.

- ImportFMA.zip - contains the files used to import data to your XenApp 7.6 farm, plus shared modules.

Module or file	Description
ImportPolicy.psm1	PowerShell script module for importing policies to XenApp 7.6.
ImportXAFarm.psm1	PowerShell script module for importing applications to XenApp 7.6
ImportPolicy.psd1	PowerShell manifest file for script module ImportPolicy.psm1.
ImportXAFarm.psd1	PowerShell manifest file for script module ImportXAFarm.psm1.

Module or file	Description
PolicyData.xsd	XML schema for policy data.
XAFarmData.xsd	XML schema for XenApp farm data.
LogUtilities.psm1	Shared PowerShell script module that contains logging functions.
XmlUtilities.psd1	PowerShell manifest file for script module XmlUtilities.psm1.
XmlUtilities.psm1	Shared PowerShell script module that contains XML functions.

Limitations

- Not all policies settings are imported; see Policy settings not imported. Settings that are not supported are ignored and noted in the log file.
- While all application details are collected in the output XML file during the export operation, only server-installed applications are imported into the XenApp 7.6 site. Published desktops, content, and most streamed applications are not supported (see the Import-XAFarm cmdlet parameters in Step-by-step: import data for exceptions).
- Application servers are not imported.
- Many application properties are not imported because of differences between the XenApp 6.x Independent Management Architecture (IMA) and the XenApp 7.6 FlexCast Management Architecture (FMA) technologies; see Application property mapping.
- A Delivery Group is created during the import. See Advanced use for details about using parameters to filter what is imported.
- Only Citrix policy settings created with the AppCenter management console are imported; Citrix policy settings created with Windows Group Policy Objects (GPOs) are not imported.
- The migration scripts are intended for migrations from XenApp 6.x to XenApp 7.6 only.
- Nested folders greater than five levels deep are not supported by Studio and will not be imported. If your application folder structure includes folders more than five levels deep, consider reducing the number of nested folder levels before importing.

Security considerations

The XML files created by the export scripts can contain sensitive information about your environment and organization, such as user names, server names, and other XenApp farm, application, and policy configuration data. Store and handle these files in secure environments.

Carefully review the XML files before using them as input when importing policies and applications, to ensure they contain no unauthorized modifications.

Policy object assignments (previously known as policy filters) control how policies are applied. After importing the policies, carefully review the object assignments for each policy to ensure that there are no security vulnerabilities resulting from the import. Different sets of users, IP addresses, or client names may be applied to the policy after the import. The allow/deny settings may have different meanings after the import.

Logging and error handling

The scripts provide extensive logging that tracks all cmdlet executions, informative messages, cmdlet execution results,

warnings, and errors.

- Most Citrix PowerShell cmdlet use is logged. All PowerShell cmdlets in the import scripts that create new site objects are logged.
- Script execution progress is logged, including the objects being processed.
- Major actions that affect the state of the flow are logged, including flows directed from the command line.
- All messages printed to the console are logged, including warnings and errors.
- Each line is time-stamped to the millisecond.

Citrix recommends specifying a log file when you run each of the export and import cmdlets.

If you do not specify a log file name, the log file is stored in the current user's home folder (specified in the PowerShell $HOME variable) if that folder exists; otherwise, it is placed in the script's current execution folder. The default log name is "XFarmYYYYMMDDHHmmSS-xxxxxx" where the last six digits constitute a random number.

By default, all progress information is displayed. To suppress the display, specify the NoDetails parameter in the export and import cmdlet.

Generally, a script stops execution when an error is encountered, and you can run the cmdlet again after clearing the error conditions.

Conditions that are not considered errors are logged; many are reported as warnings, and script execution continues. For example, unsupported application types are reported as warnings and are not imported. Applications that already exist in the XenApp 7.6 site are not imported. Policy settings that are deprecated in XenApp 7.6 are not imported.

The migration scripts use many PowerShell cmdlets, and all possible errors might not be logged. For additional logging coverage, use the PowerShell logging features. For example, PowerShell transcripts log everything that is printed to the screen. For more information, see the help for the Start-Transcript and Stop-Transcript cmdlets.

Requirements, preparation, and best practices

Important: Remember to review this entire article before beginning a migration.
You should understand basic PowerShell concepts about execution policy, modules, cmdlets, and scripts. Although extensive scripting expertise is not required, you should understand the cmdlets you execute. Use the Get-Help cmdlet to review each migration cmdlet's help before executing it. For example:

```
Get-Help -full Import-XAFarm
```

Specify a log file on the command line and always review the log file after running a cmdlet. If a script fails, check and fix the error identified in the log file and then run the cmdlet again.

Good to know:

- To facilitate application delivery while two deployments are running (the XenApp 6.x farm and the new XenApp 7.6 site), you can aggregate both deployments in StoreFront or Web Interface. See the eDocs documentation for your StoreFront or Web Interface release (Manage > Create a store).
- Application icon data is handled in one of two ways:
  - If you specify the EmbedIconData parameter in the Export-XAFarm cmdlet, exported application icon data is embedded in the output XML file.
  - If you do not specify the EmbedIconData parameter in the Export-XAFarm cmdlet, exported application icon data is stored under a folder named by appending the string "-icons" to the base name of the output XML file. For example, if the XmlOutputFile parameter is "FarmData.xml" then the folder "FarmData-icons" is created to store the application icons.
    The icon data files in this folder are .txt files that are named using the browser name of the published application

(although the files are .txt files, the stored data is encoded binary icon data, which can be read by the import script to re-create the application icon). During the import operation, if the icon folder is not found in the same location as the import XML file, generic icons are used for each imported application.

- The names of the script modules, manifest files, shared module, and cmdlets are similar. Use tab completion with care to avoid errors. For example, Export-XAFarm is a cmdlet. ExportXAFarm.psd1 and ExportXAFarm.psm1 are files that cannot be executed.
- In the step-by-step sections below, most <string> parameter values show surrounding quotation marks. These are optional for single-word strings.

For exporting from the XenApp 6.x server:

- The export must be run on a XenApp 6.x server configured with the controller and session-host (commonly known as controller) server mode.
- To run the export cmdlets, you must be a XenApp administrator with permission to read objects. You must also have sufficient Windows permission to run PowerShell scripts; the step-by-step procedures below contain instructions.
- Ensure the XenApp 6.x farm is in a healthy state before beginning an export. Back up the farm database. Verify the farm's integrity using the Citrix IMA Helper utility (CTX133983): from the IMA Datastore tab, run a Master Check (and then use the DSCheck option to resolve invalid entries). Repairing issues before the migration helps prevent export failures. For example, if a server was removed improperly from the farm, its data might remain in the database; that could cause cmdlets in the export script to fail (for example, Get-XAServer -ZoneName). If the cmdlets fail, the script fails.
- You can run the export cmdlets on a live farm that has active user connections; the export scripts read only the static farm configuration and policy data.

For importing to the XenApp 7.6 server:

- You can import data to XenApp 7.6 deployments (and later supported versions). You must install a XenApp 7.6 Controller and Studio, and create a site before importing the data you exported from the XenApp 6.x farm. Although VDAs are not required to import settings, they allow application file types to be made available.
- To run the import cmdlets, you must be a XenApp administrator with permission to read and create objects. A Full Administrator has these permissions. You must also have sufficient Windows permission to run PowerShell scripts; the step-by-step procedures below contain instructions.
- No other user connections should be active during an import. The import scripts create many new objects, and disruptions may occur if other users are changing the configuration at the same time.

Remember that you can export data and then use the -Preview parameter with the import cmdlets to see what would happen during an actual import, but without actually importing anything. The logs will indicate exactly what would happen during an actual import; if errors occur, you can resolve them before starting an actual import.

Step-by-step: export data

A video of an export walk-through is available here.

Complete the following steps to export data from a XenApp 6.x controller to XML files.

1. Download the XAMigration.zip migration tool package from the Citrix download site. For convenience, place it on a network file share that can be accessed by both the XenApp 6.x farm and the XenApp 7.6 site. Unzip XAMigration.zip on the network file share. There should be two zip files: ReadIMA.zip and ImportFMA.zip.
2. Log on to the XenApp 6.x controller as a XenApp administrator with at least read-only permission and Windows permission to run PowerShell scripts.
3. Copy ReadIMA.zip from the network file share to the XenApp 6.x controller. Unzip and extract ReadIMA.zip on the controller to a folder (for example: C:\XAMigration).

4. Open a PowerShell console and set the current directory to the script location. For example:
   `cd C:\XAMigration`
5. Check the script execution policy by running Get-ExecutionPolicy.
6. Set the script execution policy to at least RemoteSigned to allow the scripts to be executed. For example:
   `Set-ExecutionPolicy RemoteSigned`
7. Import the module definition files ExportPolicy.psd1 and ExportXAFarm.psd1:
   Import-Module .\ExportPolicy.psd1

   Import-Module .\ExportXAFarm.psd1

   Good to know:
   - If you intend to export only policy data, you can import only the ExportPolicy.psd1 module definition file. Similarly, if you intend to export only farm data, import only ExportXAFarm.psd1.
   - Importing the module definition files also adds the required PowerShell snap-ins.
   - Do not import the .psm1 script files.
8. To export policy data, run the Export-Policy cmdlet.

Parameter	Description
-XmlOutputFile "<string>.xml"	XML output file name; this file will hold the exported data. Must have an .xml extension. The file must not exist, but if a path is specified, the parent path must exist. Default: None; this parameter is required.
-LogFile "<string>"	Log file name. An extension is optional. The file is created if it does not exist. If the file exists and the NoClobber parameter is also specified, an error is generated; otherwise, the file's content is overwritten. Default: See Logging and error handling
-NoLog	Do not generate log output. This overrides the LogFile parameter if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console

Parameter	Description

Example: The following cmdlet exports policy information to the XML file named MyPolicies.xml. The operation is logged to the file named MyPolicies.log.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"
```

9. To export farm data, run the Export-XAFarm cmdlet, specifying a log file and an XML file.

Parameter	Description
-XmlOutputFile "<string>.xml"	XML output file name; this file will hold the exported data. Must have an .xml extension. The file must not exist, but if a path is specified, the parent path must exist. Default: None; this parameter is required.
-LogFile "<string>"	Log file name. An extension is optional. The file is created if it does not exist. If the file exists and the NoClobber parameter is also specified, an error is generated; otherwise, the file's content is overwritten. Default: See Logging and error handling
-NoLog	Do not generate log output. This overrides the LogFile parameter if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console
-IgnoreAdmins	Do not export administrator information. See Advanced use for how-to-use information. Default: False; administrator information is exported
-IgnoreApps	Do not export application information. See Advanced use for how-to-use information. Default: False; application information is exported

Parameter	Description
-IgnoreServers	Do not export server information. Default: False: server information is exported
-IgnoreZones	Do not export zone information. Default: False; zone information is exported.
-IgnoreOthers	Do not export information such as configuration logging, load evaluators, load balancing policies, printer drivers, and worker groups. Default: False; other information is exported Note: The purpose of the -IgnoreOthers switch is to allow you to proceed with an export when an error exists that would not affect the actual data being used for the exporting or importing process.
-AppLimit <integer>	Number of applications to be exported. See Advanced use for how-to-use information. Default: All applications are exported
-EmbedIconData	Embed application icon data in the same XML file as the other objects. Default: Icons are stored separately. See Requirements, preparation, and best practices for details
-SkipApps <integer>	Number of applications to skip. See Advanced use for how-to-use information. Default: No applications are skipped

Example: The following cmdlet exports farm information to the XML file named MyFarm.xml. The operation is logged to the file MyFarm.log. A folder named "MyFarm-icons" is created to store the application icon data files; this folder is at the same location as MyFarm.XML.

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML"
-LogFile ".\MyFarm.Log"
```

After the export scripts complete, the XML files specified on the command lines contain the policy and XenApp farm data. The application icon files contain icon data files, and the log file indicate what occurred during the export.

Step-by-step: import data

A video of an import walk-through is available here.

Remember that you can run a preview import (by issuing the Import-Policy or Import-XAFarm cmdlet with the Preview parameter) and review the log files before performing an actual import.

Complete the following steps to import data to a XenApp 7.6 site, using the XML files generating from the export.

1. Log on to the XenApp 7.6 controller as an administrator with read-write permission and Windows permission to run PowerShell scripts.
2. If you have not unzipped the migration tool package XAMigration on the network file share, do so now. Copy ImportFMA.zip from the network file share to the XenApp 7.6 Controller. Unzip and extract ImportFMA.zip on the Controller to a folder (for example: C:\XAMigration).
3. Copy the XML files (the output files generated during the export) from the XenApp 6.x controller to the same location on the XenApp 7.6 Controller where you extracted the ImportFMA.zip files.
   If you chose not to embed the application icon data in the XML output file when you ran the Export-XAFarm cmdlet, be sure to copy the icon data folder and files to the same location on the XenApp 7.6 controller as the output XML file containing the application data and the extracted ImportFMA.zip files.
4. Open a PowerShell console and set the current directory to the script location.
   `cd C:\XAMigration`
5. Check the script execution policy by running Get-ExecutionPolicy.
6. Set the script execution policy to at least RemoteSigned to allow the scripts to be executed. For example:
   `Set-ExecutionPolicy RemoteSigned`
7. Import the PowerShell module definition files ImportPolicy.psd1 and ImportXAFarm.psd1:
   Import-Module .\ImportPolicy.psd1

   Import-Module .\ImportXAFarm.psd1

   Good to know:
   - If you intend to import only policy data, you can import only the ImportPolicy.psd1 module definition file. Similarly, if you intend to import only farm data, import only ImportXAFarm.psd1.
   - Importing the module definition files also adds the required PowerShell snap-ins.
   - Do not import the .psm1 script files.
8. To import policy data, run the Import-Policy cmdlet, specifying the XML file containing the exported policy data.

Parameter	Description
-XmlInputFile "<string>.xml"	XML input file name; this file contains data collected from running the Export-Policy cmdlet. Must have an .xml extension. Default: None; this parameter is required.
-XsdFile "<string>"	XSD file name. The import scripts use this file to validate the syntax of the XML input file. See Advanced use for how-to-use information. Default: PolicyData.XSD
-LogFile "<string>"	Log file name. If you copied the export log files to this server, consider using a different log file name with the import cmdlet. Default: See Logging and error handling
-NoLog	Do not generate log output. This overrides the LogFile parameter, if it is also specified. Default: False; log output is generated

Parameter	Description
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console
-Preview	Perform a preview import: read data from the XML input file, but do not import objects to the site. The log file and console indicate what occurred during the preview import. A preview shows administrators what would happen during a real import. Default: False; a real import occurs

Example: The folowing cmdlet imports policy data from the XML file named MyPolcies.xml. The operation is logged to the file named MyPolicies.log.

```
Import-Policy -XmlInputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"
```

9. To import applications, run the Import-XAFarm cmdlet, specifying a log file and the XML file containing the exported farm data.

Parameter	Description
-XmlInputFile "<string>.xml"	XML input file name; this file contains data collected from running the Export-XAFarm cmdlet. Must have an .xml extension. Default: None; this parameter is required.
-XsdFile "<string>"	XSD file name. The import scripts use this file to validate the syntax of the XML input file. See Advanced use for how-to-use information. Default: XAFarmData.XSD
-LogFile "<string>"	Log file name. If you copied the export log files to this server, consider using a different log file name with the import cmdlet. Default: See Logging and error handling

Parameter	Description
-NoLog	Do not generate log output. This overrides the LogFile parameter, if it is also specified. Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect. Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console. Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter. Default: False; the message is printed to the console
-Preview	Perform a preview import: read data from the XML input file, but do not import objects to the site. The log file and console indicate what occurred during the preview import. A preview shows administrators what would happen during a real import. Default: False; a real import occurs
-DeliveryGroupName "<string>"	Delivery Group name for all imported applications. See Advanced use for how-to-use information. Default: "<xenapp-farm-name> - Delivery Group"
-MatchFolder "<string>"	Import only those applications in folders with names that match the string. See Advanced use for how-to-use information. Default: No matching occurs
-NotMatchFolder "<string>"	Import only those applications in folders with names that do not match the string. See Advanced use for how-to-use information. Default: No matching occurs
-MatchServer "<string>"	Import only those applications from servers whose names match the string. See Advanced use for how-to-use information.
-NotMatchServer "<string>"	Import only those applications from servers whose names do not match the string. See Advanced use for how-to-use information.

Parameter	Description
	Default: No matching occurs
-MatchWorkerGroup "<string>"	Import only those applications published to worker groups with names that match the string. See Advanced use for how-to-use information. Default: No matching occurs
-NotMatchWorkerGroup "<string>"	Import only those applications published to worker groups with names that do not match the string. See Advanced use for how-to-use information. Default: No matching occurs
-MatchAccount "<string>"	Import only those applications published to user accounts with names that match the string. See Advanced use for how-to-use information. Default: No matching occurs
-NotMatchAccount "<string>"	Import only those applications published to user accounts with names that do not match the string. See Advanced use for how-to-use information. Default: No matching occurs
-IncludeStreamedApps	Import applications of type "StreamedToClientOrServerInstalled" . (No other streamed applications are imported.) Default: Streamed applications are not imported
-IncludeDisabledApps	Import applications that have been marked as disabled. Default: Disabled applications are not imported

Example: The following cmdlet imports applications from the XML file named MyFarm.xml. The operation is logged to the file named MyFarm.log.

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"
-LogFile ".\MyFarm.Log"
```

10. After the import completes successfully, complete the post-migration tasks.

Post-migration tasks

After successfully importing XenApp 6.x policies and farm settings into a XenApp 7.6 site, use the following guidance to ensure that the data has been imported correctly.

- **Policies and policy settings**
  Importing policies is essentially a copy operation, with the exception of deprecated settings and policies, which are not imported. The post-migration check essentially involves comparing the two sides.

1. The log file lists all the policies and settings imported and ignored. First, review the log file and identify which settings and policies were not imported.
2. Compare the XenApp 6.x policies with the policies imported to XenApp 7.6. The values of the settings should remain the same (except for deprecated policy settings, as noted in the next step).
   - If you have a small number of policies, you can perform a side-by-side visual comparison of the policies displayed in the XenApp 6.x AppCenter and the policies displayed in the XenApp 7.6 Studio.
   - If you have a large number of policies, a visual comparison might not be feasible. In such cases, use the policy export cmdlet (Export-Policy) to export the XenApp 7.6 policies to a different XML file, and then use a text diff tool (such as windiff) to compare that file's data to the data in the XML file used during the policy export from XenApp 6.x.
3. Use the information in the Policy settings not imported section to determine what might have changed during the import. If a XenApp 6.x policy contains only deprecated settings, as a whole policy, it is not imported. For example, if a XenApp 6.x policy contains only HMR test settings, that policy is completely ignored because there is no equivalent setting supported in XenApp 7.6.
   Some XenApp 6.x policy settings are no longer supported, but the equivalent functionality is implemented in XenApp 7.6. For example, in XenApp 7.6, you can configure a restart schedule for Server OS machines by editing a Delivery Group; this functionality was previously implemented through policy settings.
4. Review and confirm how filters will apply to your XenApp 7.6 site versus their use in XenApp 6.x; significant differences between the XenApp 6.x farm and the XenApp 7.6 site could change the effect of filters.

- **Filters**
  Carefully examine the filters for each policy. Changes may be required to ensure they still work in XenApp 7.6 as originally intended in XenApp 6.x.

Filter	Considerations
Access Control	Access Control Should contain the same values as the original XenApp 6.x filters and should work without requiring changes.
Citrix CloudBridge	A simple Boolean; should work without requiring changes.
Client IP Address	Lists client IP address ranges; each range is either allowed or denied. The import script preserves the values, but they may require changes if different clients connect to the XenApp 7.6 VDA machines.
Client Name	Similar to the Client IP Address filter, the import script preserves the values, but they may require changes if different clients connect to the XenApp 7.6 VDA machines.
Organizational Unit	Values might be preserved, depending on whether or not the OUs can be resolved at the time they are imported. Review this filter closely, particularly if the XenApp 6.x and XenApp 7.6 machines reside in different domains. If you do not configure the filter values correctly, the policy may be applied to an incorrect set of OUs. The OUs are represented by names only, so there is a small chance that an OU name will be resolved to an OU containing different members from the OUs in the XenApp 6.x domain. Even if

Filter	Considerations
	some of the values of the OU filter are preserved, you should carefully review the values.
User or Group	Values might be preserved, depending on whether or not the accounts can be resolved at the time they are imported. Similar to OUs, the accounts are resolved using names only, so if the XenApp 7.6 site has a domain with the same domain and user names, but are actually two different domains and users, the resolved accounts could be different from the XenApp 6.x domain users. If you do not properly review and modify the filter values, incorrect policy applications can occur.
Worker Group	Worker groups are not supported in XenApp 7.6. Consider using the Delivery Group, Delivery Group Type, and Tag filters, which are supported in XenApp 7.6 (not in XenApp 6.x). • Delivery Group: Allows policies to be applied based on Delivery Groups. Each filter entry specifies a Delivery Group and can be allowed or denied. • Delivery Group Type: Allows policies to be applied based on the Delivery Group types. Each filter specifies a Delivery Group type that can be allowed or denied. • Tag: Specifies policy application based on tags created for the VDA machines. Each tag can be allowed or denied.

To recap, filters that involve domain user changes require the most attention if the XenApp 6.x farm and the XenApp 7.6 site are in different domains. Because the import script uses only strings of domain and user names to resolve users in the new domain, some of the accounts might be resolved and others might not. While there is only a small chance that different domains and users have the same name, you should carefully review these filters to ensure they contain correct values.

- **Applications**
  The application importing scripts do not just import applications; they also create objects such as Delivery Groups. If the application import involves multiple iterations, the original application folder hierarchies can change significantly.
  1. First, read the migration log files that contain details about which applications were imported, which applications were ignored, and the cmdlets that were used to create the applications.
  2. For each application:
     - Visually check to ensure the basic properties were preserved during the import. Use the information in the Application property mapping section to determine which properties were imported without change, not imported, or initialized using the XenApp 6.x application data.
     - Check the user list. The import script automatically imports the explicit list of users into the application's limit visibility list in XenApp 7.6. Check to ensure that the list remains the same.
  3. Application servers are not imported. This means that none of the imported applications can be accessed yet. The Delivery Groups that contain these applications must be assigned machine catalogs that contain the machines that have the published applications' executable images. For each application:
     - Ensure that the executable name and the working directory point to an executable that exists in the machines assigned to the Delivery Group (through the machine catalogs).
     - Check a command line parameter (which may be anything, such as file name, environment variable, or executable name). Verify that the parameter is valid for all the machines in the machine catalogs assigned to the Delivery Group.
- **Log files**
  The log files are the most important reference resources for an import and export. This is why existing log files are not

overwritten by default, and default log file names are unique.

As noted in the “Logging and error handling” section, if you chose to use additional logging coverage with the PowerShell Start-Transcript and Stop-Transcript cmdlets (which record everything typed and printed to the console), that output, together with the log file, provides a complete reference of import and export activity.

Using the time stamps in the log files, you can diagnose certain problems. For example, if an export or import ran for a very long time, you could determine if a faulty database connection or resolving user accounts took most of the time.

The commands recorded in the log files also tell you how some objects are read or created. For example, to create a Delivery Group, several commands are executed to not only create the Delivery Group object itself, but also other objects such as access policy rules that allow application objects to be assigned to the Delivery Group.

The log file can also be used to diagnose a failed export or import. Typically, the last lines of the log file indicate what caused the failure; the failure error message is also saved in the log file. Together with the XML file, the log file can be used to determine which object was involved in the failure.

After reviewing and testing the migration, you can:

1. Upgrade your XenApp 6.5 worker servers to current Virtual Delivery Agents (VDAs) by running the 7.6 installer on the server, which removes the XenApp 6.5 software and then automatically installs a current VDA. See Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS for instructions.
   For XenApp 6.0 worker servers, you must manually uninstall the XenApp 6.0 software from the server. You can then use the 7.6 installer to install the current VDA. You cannot use the 7.6 installer to automatically remove the XenApp 6.0 software.
2. From Studio in the new XenApp site, create machine catalogs (or edit existing catalogs) for the upgraded workers.
3. Add the upgraded machines from the machine catalog to the Delivery Groups that contain the applications installed on those VDAs for Windows Server OS.

Advanced use

By default, the Export-Policy cmdlet exports all policy data to an XML file. Similarly, Export-XAFarm exports all farm data to an XML file. You can use command line parameters to more finely control what is exported and imported.

- **Export applications partially** - If you have a large number of applications and want to control how many are exported to the XML file, use the following parameters:
  - AppLimit - Specifies the number of applications to export.
  - SkipApps - Specifies the number of applications to skip before exporting subsequent applications.

  You can use both of these parameters to export large quantities of applications in manageable chunks. For example, the first time you run Export-XAFarm, you want to export only the first 200 applications, so you specify that value in the AppLimit parameter.

  ```
  Export-XAFarm -XmlOutputFile "Apps1-200.xml"
  -AppLimit "200"
  ```

  The next time you run Export-XAFarm, you want to export the next 100 applications, so you use the SkipApps parameter to disregard the applications you've already exported (the first 200), and the AppLimit parameter to export the next 100 applications.

  ```
  Export-XAFarm -XmlOutputFile "Apps201-300.xml"
  -AppLimit "100" -SkipApps "200"
  ```
- **Do not export certain objects** - Some objects can be ignored and thus do not need to be exported, particularly those objects that are not imported; see Policy settings not imported and Application property mapping. Use the following

parameters to prevent exporting unneeded objects:

- IgnoreAdmins - Do not export administrator objects
- IgnoreServers - Do not export server objects
- IgnoreZones - Do not export zone objects
- IgnoreOthers - Do not export configuration logging, load evaluator, load balancing policy, printer driver, and worker group objects
- IgnoreApps - Do not export applications; this allows you to export other data to an XML output file and then run the export again to export applications to a different XML output file.

You can also use these parameters to work around issues that could cause the export to fail. For example, if you have a bad server in a zone, the zone export might fail; if you include the IgnoreZones parameter, the export continues with other objects.

- **Delivery Group names** - If you do not want to put all of your applications into one Delivery Group (for example, because they are accessed by different sets of users and published to different sets of servers), you can run Import-XAFarm multiple times, specifying different applications and a different Delivery Group each time. Although you can use PowerShell cmdlets to move applications from one Delivery Group to another after the migration, importing selectively to unique Delivery Groups can reduce or eliminate the effort of moving the applications later.
  1. Use the DeliveryGroupName parameter with the Import-XAFarm cmdlet. The script creates the specified Delivery Group if it doesn't exist.
  2. Use the following parameters with regular expressions to filter the applications to be imported into the Delivery Group, based on folder, worker group, user account, and/or server names. Enclosing the regular expression in single or double quotation marks is recommended. For information about regular expressions, see http://msdn.microsoft.com/en-us/library/hs600312(v=vs.110).aspx.
     - MatchWorkerGroup and NotMatchWorkerGroup - For example, for applications published to worker groups, the following cmdlet imports applications in the worker group named "Productivity Apps" to a XenApp 7.6 Delivery Group of the same name:
       ```
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log
       –MatchWorkerGroup ‘Productivity Apps’ –DeliveryGroupName ‘Productivity Apps’
       ```
     - MatchFolder and NotMatchFolder - For example, for applications organized in application folders, the following cmdlet imports applications in the folder named "Productivity Apps" to a XenApp 7.6 Delivery Group of the same name.
       ```
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log
       –MatchFolder ‘Productivity Apps’ –DeliveryGroupName ‘Productivity Apps’
       ```
       For example, the following cmdlet imports applications in any folder whose name contains "MS Office Apps" to the default Delivery Group.
       ```
       Import-XAFarm -XmlInputFile .\THeFarmApps.XML -MatchFolder ".*/MS Office Apps/.*"
       ```
     - MatchAccount and NotMatchAccount - For example, for applications published to Active Directory users or user groups, the following cmdlet imports applications published to the user group named "Finance Group" to a XenApp 7.6 Delivery Group named "Finance."
       ```
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log
       –MatchAccount ‘DOMAIN\\Finance Group’ –DeliveryGroupName ‘Finance’
       ```
     - MatchServer and NotMatchServer - For example, for applications organized on servers, the following cmdlet imports applications associated with the server not named "Current" to a XenApp Delivery Group named "Legacy."
       ```
       Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log
       -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'
       ```
- **Customization** - PowerShell programmers can create their own tools. For example, you can use the export script as an inventory tool to keep track of changes in a XenApp 6.x farm. You can also modify the XSD files or (create your own XSD

files) to store additional data or data in different formats in the XML files. You can specify a nondefault XSD file with each of the import cmdlets.
Note: Although you can modify script files to meet specific or advanced migration requirements, support is limited to the scripts in their unmodified state. Citrix Technical Support will recommend reverting to the unmodified scripts to determine expected behavior and provide support, if necessary.

Troubleshooting

- If you are using PowerShell verison 2.0 and you added the Citrix Group Policy PowerShell Provider snap-in or the Citrix Common Commands snap-in using the Add-PSSnapIn cmdlet, you might see the error message "Object reference not set to an instance of an object" when you run the export or import cmdlets. This error does not affect script execution and can be safely ignored.
- Avoid adding or removing the Citrix Group Policy PowerShell Provider snap-in in the same console session where the export and import script modules are used, because those script modules automatically add the snap-in. If you add or remove the snap-in separately, you might see one of the following errors:
  - "A drive with the name 'LocalGpo' already exists." This error appears when the snap-in is added twice; the snap-in attempts to mount the drive LocalGpo when it's loaded, and then reports the error.
  - "A parameter cannot be found that matches parameter name 'Controller'." This error appears when the snap-in has not been added but the script attempts to mount the drive. The script is not aware that the snap-in was removed. Close the console and launch a new session. In the new session, import the script modules; do not add or remove the snap-in separately.
- When importing the modules, if you right-click a .psd1 file and select Open or Open with PowerShell, the PowerShell console window will rapidly open and close until you stop the process. To avoid this error, enter the complete PowerShell script module name directly in the PowerShell console window (for example, Import-Module .\ExportPolicy.psd1).
- If you receive a permission error when running an export or import, ensure you are a XenApp administrator with permission to read objects (for export) or read and create objects (for import). You must also have sufficient Windows permission to run PowerShell scripts.
- If an export fails, check that the XenApp 6.x farm is in a healthy state by running the DSMAINT and DSCHECK utilities on the XenApp 6.x controller server.
- If you run a preview import and then later run the import cmdlets again for an actual migration, but discover that nothing was imported, verify that you removed the Preview parameter from the import cmdlets.

Policy settings not imported

The following computer and user policy settings are not imported because they are no longer supported. Please note, unfiltered policies are never imported. The features and components that support these settings have either been replaced by new technologies/components or the settings do not apply because of architectural and platform changes.

Computer policy settings not imported

- Connection access control
- CPU management server level
- DNS address resolution
- Farm name
- Full icon caching
- Health monitoring, Health monitoring tests
- License server host name, License server port
- Limit user sessions, Limits on administrator sessions
- Load evaluator name

- Logging of logon limit events
- Maximum percent of servers with logon control
- Memory optimization, Memory optimization application exclusion list, Memory optimization interval, Memory optimization schedule: day of month, Memory optimization schedule: day of week, Memory optimization schedule: time
- Offline app client trust, Offline app event logging, Offline app license period, Offline app users
- Prompt for password
- Reboot custom warning, Reboot custom warning text, Reboot logon disable time, Reboot schedule frequency, Reboot schedule randomization interval, Reboot schedule start date, Reboot schedule time, Reboot warning interval, Reboot warning start time, Reboot warning to users, Scheduled reboots
- Shadowing *
- Trust XML requests (configured in StoreFront)
- Virtual IP adapter address filtering, Virtual IP compatibility programs list, Virtual IP enhanced compatibility, Virtual IP filter adapter addresses programs list
- Workload name
- XenApp product edition, XenApp product model
- XML service port

* Replaced with Windows Remote Assistance

User policy settings not imported

- Auto connect client COM ports, Auto connect client LPT ports
- Client COM port redirection, Client LPT port redirection
- Client printer names
- Concurrent logon limit
- Input from shadow connections *
- Linger disconnect timer interval, Linger terminate timer interval
- Log shadow attempts *
- Notify user of pending shadow connections *
- Pre-launch disconnect timer interval, Pre-launch terminate timer interval
- Session importance
- Single Sign-On, Single Sign-On central store
- Users who can shadow other users, Users who cannot shadow other users *

* Replaced with Windows Remote Assistance

Application types not imported

The following application types are not imported.

- Server desktops
- Content
- Streamed applications (App-V is the new method used for streaming applications)

Application property mapping

The farm data import script imports only applications. The following application properties are imported without change.

IMA Property	FMA Property
AddToClientDesktop	ShortcutAddedToDesktop

IMA Property	FMA Property
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
Description	Description
DisplayName	PublishedName
Enabled	Enabled
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

Note: IMA and FMA have different restrictions on folder name length. In IMA, the folder name limit is 256 characters; the FMA limit is 64 characters. When importing, applications with a folder path containing a folder name of more than 64 characters are skipped. The limit applies only to the folder name in the folder path; the entire folder path can be longer than the limits noted. To avoid applications from being skipped during the import, Citrix recommends checking the application folder name length and shortening it, if needed, before exporting.

The following application properties are initialized or uninitialized by default, or set to values provided in the XenApp 6.x data:

FMA Property	Value
Name	Initialized to the full path name, which contains the IMA properties FolderPath and DisplayName, but stripped of the leading string "Applications\"
ApplicationType	HostedOnDesktop
CommandLineArguments	Initialized using the XenApp 6.x command line arguments
IconFromClient	Uninitialized; defaults to false
IconUid	Initialized to an icon object created using XenApp 6.x icon data

FMA Property	Value
SecureCmdLineArgumentsEnabled	Uninitialized; defaults to true
UserFilterEnabled	Uninitialized; defaults to false
UUID	Read-only, assigned by the Controller
Visible	Uninitialized; defaults to true

The following application properties are partially migrated:

IMA Property	Comments
FileTypes	Only the file types that exist on the new XenApp site are migrated. File types that do not exist on the new site are ignored. File types are imported only after the file types on the new site are updated.
IconData	New icon objects are created if the icon data has been provided for the exported applications.
Accounts	The user accounts of an application are split between the user list for the Delivery Group and the application. Explicit users are used to initialize the user list for the application. In addition, the "Domain Users" account for the domain of the user accounts is added to the user list for the Delivery Group.

The following XenApp 6.x properties are not imported:

IMA Property	Comments
ApplicationType	Ignored.
HideWhenDisabled	Ignored.
AccessSessionConditions	Replaced by Delivery Group access policies.
AccessSessionConditionsEnabled	Replaced by Delivery Group access policies.
ConnectionsThroughAccessGatewayAllowed	Replaced by Delivery Group access policies.
OtherConnectionsAllowed	Replaced by Delivery Group access policies.
AlternateProfiles	FMA does not support streamed applications.
OfflineAccessAllowed	FMA does not support streamed applications.

IMA Property	Comments
ProfileLocation	FMA does not support streamed applications.
ProfileProgramArguments	FMA does not support streamed applications.
ProfileProgramName	FMA does not support streamed applications.
RunAsLeastPrivilegedUser	FMA does not support streamed applications.
AnonymousConnectionsAllowed	FMA uses a different technology to support unauthenticated (anonymous) connections.
ApplicationId, SequenceNumber	IMA-unique data.
AudioType	FMA does not support advanced client connection options.
EncryptionLevel	SecureICA is enabled/disabled in Delivery Groups.
EncryptionRequired	SecureICA is enabled/disabled in Delivery Groups.
SslConnectionEnabled	FMA uses a different SSL implementation.
ContentAddress	FMA does not support published content.
ColorDepth	FMA does not support advanced window appearances.
MaximizedOnStartup	FMA does not support advanced window appearances.
TitleBarHidden	FMA does not support advanced window appearances.
WindowsType	FMA does not support advanced window appearances.
InstanceLimit	FMA does not support application limits.
MultipleInstancesPerUserAllowed	FMA does not support application limits.
LoadBalancingApplicationCheckEnabled	FMA uses a different technology to support load balancing.
PreLaunch	FMA uses a different technology to support session prelaunch.

IMA Property	Comments
CachingOption	FMA uses a different technology to support session prelaunch.
ServerNames	FMA uses a different technology.
WorkerGroupNames	FMA does not support worker groups.

Migrate XenDesktop 4

Jul 07, 2014

You can transfer data and settings from a XenDesktop 4 farm to a XenDesktop 7.x Site using the Migration Tool, which is available in the Support > Tools > MigrationTool folder on the XenDesktop installation media. The tool includes:

- The export tool, XdExport, which exports XenDesktop 4 farm data to an XML file (default name: XdSettings.xml). The XML file schema resides in the file XdFarm.xsd.
- The import tool, XdImport, which imports the data by running the PowerShell script Import-XdSettings.ps1.

To successfully use the Migration Tool, both deployments must have the same hypervisor version (for example, XenServer 6.2), and Active Directory environment.

You cannot use this tool to migrate XenApp, and you cannot migrate XenDesktop 4 to XenApp.

Tip: You can upgrade XenDesktop 5 (or later XenDesktop versions) to the current XenDesktop version; see Upgrade a deployment.

Limitations

Not all data and settings are exported. The following configuration items are not migrated because they are exported but not imported:

- Administrators
- Delegated administration settings
- Desktop group folders
- Licensing configuration
- Registry keys

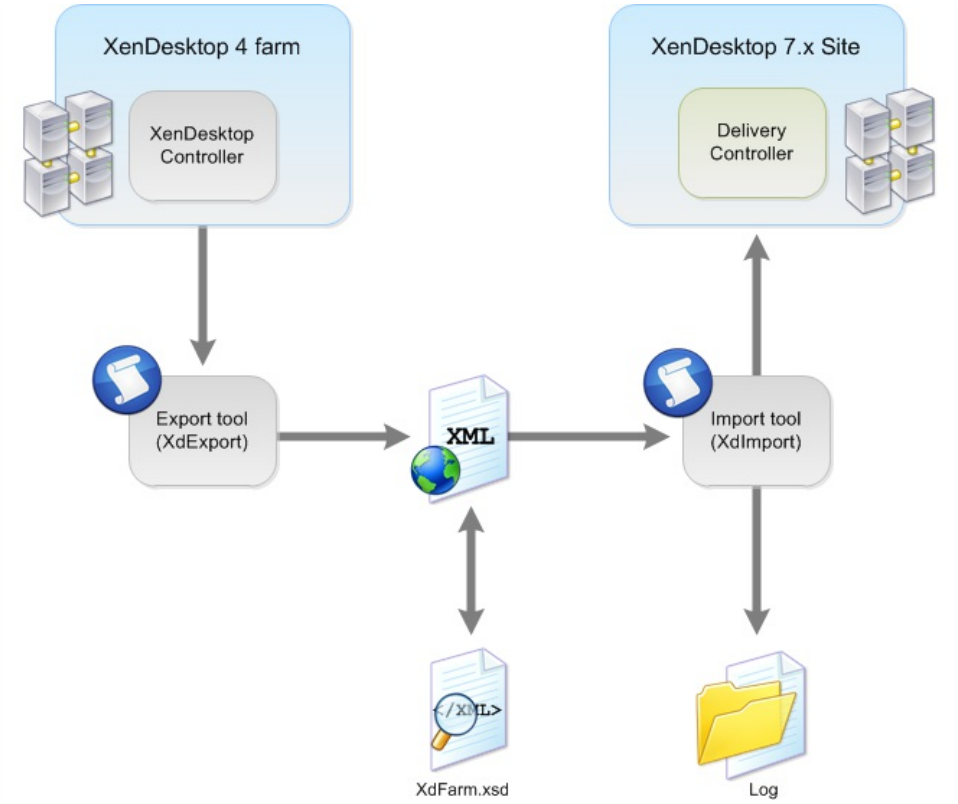
These use cases are not directly supported in migration:

- Merging settings of policies or desktop group or hosting settings.
- Merging private desktops into random Delivery Groups.
- Adjusting existing component settings through the migration tools.

For more information, see What is and is not migrated .

Migration steps

The following figure summarizes the migration process.



The migration process follows this sequence:

1. In the Studio console on the XenDesktop 4 Controller, turn on maintenance mode for all machines to be exported.
2. Export data and settings from your XenDesktop 4 farm to an XML file using XdExport; see Export from a XenDesktop 4 farm.
3. Edit the XML file so that it contains only the data and settings you want to import into your new XenDesktop Site; see Edit the Migration Tool XML file.
4. Import the data and settings from the XML file to your new XenDesktop Site using XdImport; see Import XenDesktop 4 data.
5. To make additional changes, repeat steps 3 and 4. After making changes, you might want to import additional desktops into existing Delivery Groups. To do so, use the Mergedesktops parameter when you import.
6. Complete the post-migration tasks; see Post-migration tasks.

Before migrating

Complete the following before beginning a migration:

- Make sure you understand which data can be exported and imported, and how this applies to your own deployment. See What is and is not migrated.
- Citrix strongly recommends that you manually back up the Site database so that you can restore it if any issues are discovered.
- Install the XenDesktop 7.x components and create a Site, including the database.
- To migrate from XenDesktop 4 , all VDAs must be at a XenDesktop 5.x level so that they are compatible with both XenDesktop 4 and XenDesktop 7.x controllers. After the Controller infrastructure is fully running XenDesktop 7.x, Windows 7 VDAs can be upgraded to XenDesktop 7.x. For details, see Migration examples.

Export from a XenDesktop 4 farm

Jul 07, 2014

The export tool, XdExport, extracts data from a single XenDesktop 4 farm and produces an XML file from representations of the data values.

The schema of the XML file resides in the file XdFarm.xsd, which is included in the migration tool download XdExport.zip and XdImport.zip.

Run XdExport on a XenDesktop 4 Controller in the farm from which you want to export data. This machine must have the XenDesktop 4 PowerShell SDK installed. You must have the following permissions to export the data:

- The user identity of at least read-only Citrix administrator of the farm.
- Permission to read the registry.

Although not recommended, you can run the tool while the XenDesktop Controller is in active use (for example, users are logged in to VDAs).

Citrix strongly recommends:

- The XenDesktop 4 Controller on which you run the tool be up-to-date with public hotfixes.
- Not making configuration changes to the Site while the export is running (for example, removing Desktop Groups).

1. Download XdExport.zip and extract the files to the XenDesktop 4 Controller.
2. At a command line prompt, run XdExport.exe with the following optional parameters:

Parameter	Description
-Verbose	Generates messages providing detailed progress information.
-FilePath <path>	Indicates the location of the XML file to which the farm data is exported. Default = .\XdSettings.xml
-Overwrite	Overwrites any file existing in the location specified in -FilePath. If you do not supply this parameter and an output file already exists, the tool fails with the message "Error: File already exists. Specify -Overwrite to allow the file to be overwritten. "
-? or -help	Displays text describing the parameters and exits without exporting any data.

3. If the tool runs successfully, the message Done appears. The XdSettings.xml file resides in the location specified in the FilePath parameter. If the tool fails, an error message appears.

Edit the Migration Tool XML file

Jul 07, 2014

Before importing data to a XenDesktop 7.x Site, check and edit the contents of the XML file generated by the export tool (XdExport), particularly if you migrate in multiple stages and import some users, Delivery Groups, and policies before importing others.

Use any text editor to view or change the file contents; you can use a specialized XML editor such as Microsoft XML Notepad.

Some elements within the XML content must be present for the XML file to be accepted by the import tool (XdImport).

The required XML schema is defined in the XdFarm.xsd file that is supplied as part of the Migration Tool download. When working with this file:

- A minOccurs attribute with a value of 1 or more indicates that particular elements must be present if the parent element is present.
- If the XML file supplied to the Import tool is not valid, the tool halts and an error message appears that should enable you to locate where the problem lies in the XML file.

Import a subset of desktops or Delivery Groups

To import only a subset of Delivery Groups and desktops, edit the contents of the DesktopGroups element. The DesktopGroups element can hold many DesktopGroup elements, and within each DesktopGroup element there is a Desktops element that can contain many Desktop elements.

Do not delete the DesktopGroups element, although you can delete all the DesktopGroup elements and leave it empty. Similarly, within each DesktopGroup element, the Desktops element must be present but can be empty of Desktop elements.

Delete Desktop or DesktopGroup elements to avoid importing particular single machines or entire Delivery Groups. For example, the XML file contains:

```
<DesktopGroups>
 <DesktopGroup name="Group1">
…
  <Desktops>
   <Desktop sameName="DOMAIN\MACHINE1$">
…
   </Desktop>
  </Desktops>
…
 </DesktopGroup>
 <DesktopGroup name="Group2">
…
  <Desktops>
   <Desktop samName="DOMAIN\MACHINE2$">
…
   </Desktop>
   <Desktop samName="DOMAIN\MACHINE3$">
…
```

```
  </Desktop>
 </Desktops>
...
</DesktopGroup>
</DesktopGroups>
```

In this example, the edits prevent Group1 group from being imported. Only Machine3 from the Group2 group will be imported:

```
<DesktopGroups>
 <DesktopGroup name="Group2">
...
 <Desktops>
  <Desktop samName="DOMAIN\MACHINE3$">
...
  </Desktop>
 </Desktops>
...
 </DesktopGroup>
</DesktopGroups>
```

Manage Delivery Groups with duplicate names

In XenDesktop 4, Desktop Groups can be organized in folders, Desktop Groups with the same name can appear in different folders, and the internal desktop group name is the name that appears to users. In this release, Delivery Groups cannot be placed in folders, and each Delivery Group must have a unique internal name, and the name that appears to users can be different from the internal name. To accommodate these differences, you might have to rename Desktop Groups.

For example, in your XenDesktop 4 farm, you could have two different Desktop Groups that appear with the name "My Desktop" to two different users, and you could use Desktop Groups folders to achieve this. If these Delivery Groups are to remain separate in the XenDesktop 7.x Site, you must edit the Desktop Group names in the XML file to make them unique.

If a Delivery Group in the XenDesktop 7.x Site has the same name as a Desktop Group to be imported, and the Delivery Groups are to remain separate in the XenDesktop 7.x Site, you must edit the XenDesktop 4 Desktop Group name in the XML file to keep the name unique in the Site. If the Desktop Group to be imported is really the same as the XenDesktop 7.x Delivery Group, and the machines in the XML file are to be merged into the existing Desktop Group, you do not need to rename the Desktop Group; instead, specify the -MergeDesktops parameter to the Import tool. For example, if the XML file contains:

```
<DesktopGroups>
 <DesktopGroup name="My Desktop">
...
 <Folder>\Sales</Folder>
</DesktopGroup>
 <DesktopGroup name="My Desktop">
...
 <Folder>\Finance</Folder>
</DesktopGroup>
</DesktopGroups>
```

Remove the duplicate names as follows:

```
<DesktopGroups>
 <DesktopGroup name="Sales Desktops">
...
```

```
  <Folder>\Sales</Folder>
 </DesktopGroup>
 <DesktopGroup name="Finance Desktops">
...
  <Folder>\Finance</Folder>
 </DesktopGroup>
</DesktopGroups>
```

Manage policy imports

You can delete policies from the XML file, and you can specify unique names to avoid policy name duplication. There is no support for merging policies.

- When you import policy data, either all polices are imported successfully or, if there is any failure, no policy data is imported.
- Importing large numbers of policies with many settings can take several hours.
- If you import policies in batches, their original prioritization may be affected. When you import policies, the relative priorities of the imported polices are maintained, but they are given higher priority than policies already in the Site. For example, if you have four polices to import with priority numbers 1 to 4, and you decide to import them in two batches, you should import policies with priorities 3 and 4 first, because the second batch of policies automatically gets higher priority.

To import only a subset of policies into the XenDesktop 7.x Site, edit the contents of the Policies element. The Policies element can hold many Policy elements. You must not delete the Policies element, although you can delete all the Policy elements and leave it empty. Delete entire Policy elements to avoid importing particular XenDesktop 4 farm policies. For example, if the XML file contains:

```
<Policies>
 <Policy name="Sales Policy">
...
 </Policy>
...
</Policies>
```

To avoid importing any XenDesktop 4 policies, and avoid clashes with policies already configured in the XenDesktop 7.x Site, edit the file to remove the individual Policy elements as follows:

```
<Policies>
</Policies>
```

Alternatively, edit the file so that the policy is imported with a different name as follows:

```
<Policies>
 <Policy name="XD4 Sales Policy">
...
 </Policy>
...
</Policies>
```

Import XenDesktop 4 data

Jul 07, 2014

The import tool, XdImport, reads settings from XenDesktop 4 that are contained in the XML file produced by the export tool, XdExport, and applies those settings to an existing XenDesktop 7.x Site. The Import tool uses the PowerShell script Import-XdSettings.ps1.

To apply only a subset of the exported data, edit the XML file before running the Import tool. For example, you might want to remove desktop groups and policies that are not needed in your XenDesktop 7.x deployment. The import tool runs successfully if you leave entire elements empty. For example, you can delete all the desktop groups without causing any issues. The tool always validates the XML file before attempting to import any data.

Run XdImport on any machine on which all the XenDesktop 7.x SDKs are installed. You must be a Full XenDesktop administrator identity to run the tool.

Before you import, make sure that you have set up a XenDesktop 7.x Site, including its database. Citrix recommends that you complete the import to XenDesktop 7.x before any user testing or general Site configuration occurs. Merge configurations only when the Site is not in use.

1. Create a XenDesktop 7.x Site.
2. Download XdImport.zip and extract the files to the machine where you will run the tool.
3. In a PowerShell session, run Import-XdSettings.ps1 with the following parameters:

Parameter	Description

-HypervisorConnectionCredentials	(Required.) A PowerShell hash table that maps Hypervisor addresses to PSCredential instances as required for the creation of Hypervisor connections. Default = @{}
	
	Enter credentials for the Hypervisor to which the XenDesktop 4 farm connects.
	
	For a single Hypervisor, create the argument as follows:
	
	`$credential = Get-Credential`
	`$mappings = @{"http://<HypervisorIP>"`
	`=$credential}`
	`.\Import-XdSettings.ps1`
	`-FilePath. \XdSettings.xml`
	`-HypervisorConnectionCredentials $mappings`
	The address specified in the hash table must exactly match the address in the XML file.
	
	For example, with both a XenServer and a VMware hypervisor, create the following argument:
	
	`$Xencredential = Get-Credential`
	`$VMWcredential = Get-Credential`
	`$mappings = @{"http://<XenHypervisorIP>"`
	`= $Xencredential;"http://<VmWHypervisorIP>/SDK"`

Parameter	Description
	= $VMWcredential} .\Import-XdSettings.ps1 -FilePath. \XdSettings.xml -HypervisorConnectionCredentials $mappings
-FilePath <path>	(The value for <path> is required.) The location of the XML file from which the farm data is to be imported.
-AdminAddress	The name of a Controller in the XenDesktop 7.x Site. Default = localhost
-MergeDesktops	Adds desktops defined in the XML file to Delivery Groups in the XenDesktop 7.x Site that have the same name as the groups described in the XML file. The associated machines and users are also added. If this parameter is not supplied, no content is added to existing Delivery Groups in the XenDesktop 7.x Site.
-SkipMachinePolicy	The script does not create a machine policy that contains site-level settings. If you do not supply this parameter and the machine policy for the Site exists, the script fails.
-WhatIf	Completes a trial run to determine what would be changed in or added to the XenDesktop 7.x Site. Including this parameter sends the information to the log file, but does not change the Site.
-LogFilePath <path>	Indicates the full path of the log file. The log file contains text describing all writes performed against the XenDesktop 7.x Site. Default = .\Import-XdSettings.log
-? or -help	Displays information about parameters and exits without importing any data.

If the XML file contains policy data, either all polices are imported successfully or if there is any failure, no policy data is imported. Importing large numbers of policies with many settings can take several hours.

When the script completes, the message Done appears. After successfully importing the data from the XML file, you can either run further export and import iterations, or if you have imported all the relevant data, complete the post-migration tasks.

Post-migration tasks

Jul 07, 2014

After successfully importing data from a XenDesktop 4 farm to a XenDesktop 7.x Site, complete the following tasks before using the new Site for production work:

- Upgrade the Virtual Delivery Agents (VDAs). Although it is not required, Citrix recommends that you upgrade VDAs before upgrading Controllers, Studio, or Director.
  - For Windows Vista and Windows XP, upgrade to XenDesktop 5. 6 Feature Pack 1 Virtual Desktop Agent.
  - For Windows 7, upgrade to the XenDesktop 7.x Virtual Delivery Agent.
- Create administrators you need for the XenDesktop 7.x Site.
- Update user devices — Citrix recommends that you update user devices with the latest version of Citrix Receiver to benefit from hotfixes and to receive support for the latest features.
- Modify the imported desktops to use registry-based Controller discovery, and point them to the XenDesktop 7.x Controllers using one of the following methods:
  - Manually edit the registry to remove the unnecessary Organizational Unit (OU) GUID registry entry, and add a ListOfDDCs registry entry.
  - Set up a machine policy to distribute the list of Controllers to the desktops, using the Active Directory policy GPMC.msc. You cannot use Studio to configure this setting.

  Registry-based Controller discovery is the default for XenDesktop 7.x, but Active Directory-based discovery is still available.

- Optionally, implement the following registry key settings described in the best practices for XenDesktop registry-based registration in CTX133384:
  - HeartbeatPeriodMS
  - PrepareSessionConnectionTimeoutSec
  - MaxWorkers
  - DisableActiveSessionReconnect
  - ControllersGroupGuid

  If you do not perform this action, the default XenDesktop 7.x settings for these keys are used.

- Turn off maintenance mode for the imported machines if they were in maintenance mode in XenDesktop 4 before the XML file was generated.
- Check the XenDesktop 7.x settings to make sure that they are correct, particularly if you had changed the PortICAConfig XML file on XenDesktop 4.
- Review all migrated components to make sure that the migration was successful.

Migration examples

Nov 18, 2014

Example 1: Single large-scale XenDesktop 4 farm to a XenDesktop 7 Site

In this example, a XenDesktop 4 farm is in use. The XenDesktop 4 farm has 50 desktop groups, where each group contains an average 100 desktops. The XenDesktop 4 desktops are provided through Provisioning Services (PVS), and the machines are running on VMware ESX hypervisors. The VDA installed on all the VMs is the XenDesktop version 4.

Migration steps

1. Upgrade all XenDesktop 4 VDAs to XenDesktop 5.6 Feature Pack 1 VDA software. This allows the VDAs to register with both the XenDesktop 4 controller and the XenDesktop 7 Delivery Controller.
   - For Windows 7 VDAs, see Upgrading the Virtual Desktop Agent on a VM or Blade Computer.
   - For Windows XP and Windows Vista VDAs, see Virtual Desktop Agents on Windows XP or Windows Vista.
2. Make sure that all users log off the XenDesktop 4 farm.
3. Make sure that all these machines are in maintenance mode.
4. Run the export tool (XdExport) on the XenDesktop 4 farm.
5. Install XenDesktop 7 components.
   1. Use Studio to create a full production mode Site.
   2. If Provisioning Services is part of the deployment, upgrade the Provisioning Services server and agents.
   3. Upgrade the License Server and associated licenses.
6. Unzip the Import Tool (XdImport) to a local directory on the XenDesktop 7 Controller.
7. Copy the XML file (XdSettings.xml) generated in Step 4 by the export tool to the local directory.
8. From the PowerShell console of the Studio root node on the XenDesktop 7 Site, start a PowerShell session.
9. Run the import tool (XdImport), passing the credentials of the associated hypervisors and the path of the XML file.
10. Manually recreate administrator settings from the Administrator node in the Studio navigation pane; see Delegated Administration for details.
11. Modify the imported desktops to use registry-based Controller discovery; and point them to the new XenDesktop 7 Controller.
12. For VDAs running on Windows 7, Citrix recommends you upgrade those VDAs to use the XenDesktop 7 VDA for Windows Desktop OS, which provides access to all new features.
    After upgrading the VDAs to XenDesktop 7 for machines in a catalog or Delivery Group, upgrade the catalog (see Manage machine catalogs) and Delivery Groups (see Manage settings in Delivery Groups).
13. Turn off maintenance mode for the Delivery Groups.
14. Configure StoreFront to provide the desktops formerly provided through Web Interface. See the StoreFront documentation.

Example 2: XenDesktop 4 farm export with a partial import to XenDesktop 7.1 Site

In this example, the migration occurs in a number of steps, each step migrating a subset of the remaining desktops. A XenDesktop 4 farm is in use, and a XenDesktop 7.1 Site has already been created and is in use. The XenDesktop 4 farm has 50 desktop groups, and each group contains an average 100 desktops. The XenDesktop 4 desktops are provided through Provisioning Services, and the machines are running on Citrix XenServer hypervisors. The VDA installed on all the VMs is the XenDesktop version 4.

Migration steps

1. Run the export tool on the XenDesktop 4 farm.
    1. Unzip the Export Tool (XdExport) on one of the Desktop Delivery Controllers in the farm.
    2. As a Citrix Administrator, run the export tool with no parameters.
2. Copy and edit the resulting XML file so that it contains only the groups and desktops that you want to migrate.
3. In the XenDesktop 4 farm, make sure that all users on desktops to be migrated have logged off and turn on maintenance mode for all desktops that are to be migrated.
4. Unzip the Import Tool (XdImport) to a local directory on the XenDesktop 7.1 Delivery Controller.
5. Copy the edited XML to the local directory.
6. From the PowerShell console of the Studio root node on the XenDesktop 7.1 Site, start a PowerShell session.
7. Run the Import Tool (XdImport), passing the credentials of the associated hypervisors and the path of the XML file.
8. Manually recreate Administrator settingsf rom the Administrator node in the Studio navigation pane; see Delegated Administration for details.
9. Modify the imported desktops to use registry-based Controller discovery; and point them to the new XenDesktop 7.1 Controller.
10. Upgrade all VDAs to the appropriate VDA software:
    - For Windows 7 VDAs:
        - Upgrade to XenDesktop 7 Virtual Delivery Agents as described in Upgrading the Virtual Desktop Agent on a VM or Blade Computer
        - After upgrading all VDA software to XenDesktop 7 for machines in a catalog or Delivery Group, upgrade the catalog (see Manage machine catalogs) and Delivery Groups (see Manage settings in Delivery Groups).
    - For Windows XP and Windows Vista VDAs, upgrade to XenDesktop 5.6 FP1; see Virtual Desktop Agents on Windows XP or Windows Vista.
11. Turn off maintenance mode for the Delivery Groups.
12. Configure StoreFront to provide the desktops formerly provided through Web Interface. See the StoreFront documentation.

What is and is not migrated

Apr 27, 2015

What is migrated

Although not all inclusive, the following table describes what happens to the most significant data during migration to this release. Unless noted, the data type is imported.

Data type	Notes
Desktop Groups	Desktop Groups become Delivery Groups in this release. Desktop Group icons are not exported. SecureIcaRequired is set to True if the DefaultEncryptionLevel in XenDesktop 4 is not Basic. If a Desktop Group in the XenDesktop 4 farm has the same name as a Delivery Group in the XenDesktop 7.x Site, you can add desktops belonging to the XenDesktop 4 group to a Delivery group of the same name in the target Site. To do this, specify the MergeDesktops parameter when you run the import tool. The settings of the XenDesktop 7.x Delivery Group are not overwritten with the settings of the XenDesktop 4 group. If this parameter is not specified and there is a group with the same name as one defined in the XML file, the tool displays an error and stops before any data is imported.
Desktops	You cannot add private desktops to a random Delivery Group. Random desktops cannot be added to a static Delivery Group.
Machines	Machines are imported into four machine catalogs. The following machine catalogs are automatically created in the XenDesktop 7.x Site by the import tool: • Imported existing random (for pooled VMs) • Imported existing static (for assigned VMs) • Imported physical random (for pooled PCs or blades) • Imported physical static (for private PCs or blades). Any subsequent import of machines uses the same four machine catalogs.
Pool management pools	Includes multi-pool pools, and idle pool settings including schedule. • PeakBuffersizePercent is set to 10% by default. • OffPeakBufferSizePercent is set to 10% by default. • Any unselected days in the Business days setting on XenDesktop 4 are imported as part of the Weekend power time scheme in this release. • HostingXD4 action times are rounded up to the nearest minute. • Start times are rounded down to the nearest hour. • End times are rounded up to the nearest hour.
Farm settings	The following farm settings are imported as a Machine policy: • IcaKeepAlive

Data type	Notes
	• AutoClientReconnect • SessionReliability The setting to enable Flash player is not imported.
Policies	Some policy data is imported. Filters, settings, and printers are imported as User policies. For further details of user policy export and import, see the other table in this document. • New access policy rules are created from XenDesktop 4 group settings. • When policies are imported, their relative priority order is preserved. However, they are always added with a higher priority than any existing policies on the XenDesktop 7.x Site. • Policy merging is not supported. There is no option to import policies into Active Directory. They are always stored in the Site.
User assignments	
Hypervisor settings	This parameter is required with the XdImport tool. Hypervisor addresses are exported, but not the credentials required to access those hypervisors. To create hypervisor connections in the XenDesktop 7.x Site, extract the addresses from the XML file and create a PowerShell hash table that maps them to the relevant credential instances. Then specify this hash table in the import tool HypervisorConnectionCredentials parameter. For further details, see Import XenDesktop 4 data Merging or updating hypervisor settings for existing Desktop Groups and hypervisor connections is not supported.
Administrators	(Not imported.) No administrator data is imported, including data about delegated administrators. You create new administrators for your XenDesktop 7.x Site.
Licensing configuration	(Not imported.) Includes information such as the License Server name and edition. License files are not exported.
Desktop Group folders	(Not imported.) This release does not support Desktop Group folders. If there are duplicate Desktop Group names (because different folders in the XenDesktop 4 farm contained groups with the same names) and you do not edit names in the XML file, the Import Tool halts.
Registry keys	(Not imported.) For information on implementing registry keys, see Post-migration tasks.

User policy data

The following table describes how User policy data is exported and imported.

XenDesktop 4 category and setting	XML file	XenDesktop 7.x category and setting
Bandwidth\Visual Effects\Session Limits OEM Virtual Channels	ClientOEMVCBandwidth	Not imported
Client Devices\Resources\Other Turn off OEM virtual channels	DisableOEMVirtualChannels	Not imported
User Workspace\Time Zones Do not use client's local time	DoNotUseClientLocalTime	Not imported
Security\Encryption SecureICA encryption	ClientSecurityRequirement	Not imported
Bandwidth\SpeedScreen Image acceleration using lossy compression	LossyCompression settings	ICA\Visual Display\Still Images Lossy compression level Lossy compression threshold value Heavyweight compression ICA\Visual Display\Moving Images Progressive compression level Progressive compression threshold value
Bandwidth\Visual Effects Turn off desktop wallpaper	TurnOffWallpaper	ICA\Desktop UI Desktop wallpaper
Bandwidth\Visual Effects Menu animation	TurnOffMenuWindowAnimation	ICA\Desktop UI Menu animation

XenDesktop 4 category and setting	XML file	XenDesktop 7.x category and setting
Bandwidth\Visual Effects Turn off window contents while dragging	DoNotShowWindowContentsWhileDragging	ICA\Desktop UI View window contents while dragging
Bandwidth\Visual Effects\Session Limits Audio	ClientAudioBandwidth__AllowedBandWidth	ICA\Bandwidth Audio redirection bandwidth limit
Bandwidth\Visual Effects\Session Limits Clipboard	ClientClipboardBandwidth__AllowedBandWidth	ICA\Bandwidth Clipboard redirection bandwidth limit
Bandwidth\Visual Effects\Session Limits COM Ports	ClientComBandwidth__AllowedBandWidth	COM port redirection is deprecated in XenDesktop 7.x
Bandwidth\Visual Effects\Session Limits Drives	ClientDriveBandwidth__AllowedBandWidth	ICA\Bandwidth File redirection bandwidth limit
Bandwidth\Visual Effects\Session Limits LPT Ports	ClientLptBandwidth__AllowedBandWidth	LPT port redirection is deprecated in XenDesktop 7.x
Bandwidth\Visual Effects\Session Limits Overall Session	OverallBandwidth__AllowedBandWidth	ICA\Bandwidth Overall session bandwidth limit
Bandwidth\Visual Effects\Session Limits Printer	LimitPrinterBandWidth__AllowedBandWidth	ICA\Bandwidth Printer redirection bandwidth limit
Client Devices\Resources\Audio Microphones	ClientAudioMicrophone__TurnOn	ICA\Audio Client microphone redirection

XenDesktop 4 category and setting	XML file	XenDesktop 7.x category and setting
Client Devices\Resources\Audio Sound Quality	ClientAudioQuality__Quality	ICA\Audio Audio quality
Client Devices\Resources\Audio Turn off speakers	DisableClientAudioMapping	ICA\Audio Client audio redirection
Client Devices\Resources\Drives Connection	ConnectClientDriveAtLogon__TurnOn	ICA\File Redirection Auto connect drives
Client Devices\Resources\Drives Turn off Floppy disk drives	DisableClientDriveMapping__DisableFloppyDrive	ICA\File Redirection Client floppy drives
Client Devices\Resources\Drives Turn off Hard drives	DisableClientDriveMapping__DisableHardDrive	ICA\File Redirection Client fixed drives
Client Devices\Resources\Drives Turn off CD-ROM drives	DisableClientDriveMapping__DisableCdrom	ICA\File Redirection Client optical drives
Client Devices\Resources\Drives Turn off Remote drives	DisableClientDriveMapping__DisableRemote	ICA\File Redirection Client network drives
Client Devices\Resources\Drives Turn off USB disk drives	DisableClientDriveMapping__DisableUSB	ICA\File Redirection Client removable drives
Client Devices\Resources\Drives\Optimize Asynchronous writes	CDMAsyncWrites	ICA\File Redirection User asynchronous writes
Client Devices\Resources\Other Turn off clipboard mapping	DisableClientClipboardMapping	ICA Client clipboard redirection
Client Devices\Resources\Ports Turn off COM ports	DisableClientCOMPortMapping	COM port redirection is deprecated in XenDesktop 7.x
Client Devices\Resources\Ports	DisableClientLPTPortMapping	LPT port redirection is

XenDesktop 4 category and setting	XML file	XenDesktop 7.x category and setting
Turn off LPT ports		deprecated in XenDesktop 7.x
Client Devices\Resources\USB USB	RemoteUSBDevices__DisableRemoteUSBDevices	ICA\USB Devices Client USB device redirection
Printing\Client Printers Auto-creation	ConnectClientPrinterAtLogon__Flag	ICA\Printing\Client Printers Auto-create client printers
Printing\Client Printers Legacy client printers	LegacyClientPrinters__TurnOn	ICA\Printing\Client Printers Client printer names
Printing\Client Printers Printer properties retention	ModifiedPrinterProperties__WriteMethod	ICA\Printing\Client Printers Printer properties retention
Printing\Client Printers Print job routing	ClientPrintingForNetworkPrinter__TurnOn	ICA\Printing\Client Printers Direct connections to print servers
Printing\Client Printers Turn off client printer mapping	DisableClientPrinterMapping	ICA\Printing Client printer redirection
Printing\Drivers Native printer driver auto-install	PrintDriverAutoInstall__TurnOn	ICA\Printing\Drivers Automatic installation of inbox printer drivers
Printing\Drivers Universal driver	ClientPrintDriverToUse	ICA\Printing\Drivers Universal print driver use
Printing\Session printers Session printers	NetworkPrinters	ICA\Printing Session printers
Printing\Session printers Choose client's default printer	DefaultToMainClientPrinter__NetworkDefault DefaultToMainClientPrinter__TurnOn	ICA\Printing Default printer

What is not migrated

Not all XenDesktop 4 components are supported in this release. The following items are not migrated:

- **Virtual Delivery Agent** - Before a XenDesktop 7.x Delivery Controller can manage virtual desktops from XenDesktop 4, you must upgrade the VDAs to a minimum release of XenDesktop 5.x. For information about upgrading VDAs, see Post-migration tasks.
- **Controllers** - You must deploy new Controller servers. You cannot upgrade a XenDesktop 4 Controller to a XenDesktop 7.x Site. XenDesktop 7.x Sites cannot join a XenDesktop 4 farm, and XenDesktop 4 Controllers cannot join a XenDesktop 7.x Site. In addition, each version has different server requirements; XenDesktop 4 requires Windows Server 2003 and XenDesktop 7.x requires later Windows Server versions.
- **Web Interface** - Citrix recommends using StoreFront with XenDesktop 7.x. See the StoreFront documentation for installation and setup details. When the XenDesktop installer detects Web Interface, it installs StoreFront, but does not remove Web Interface.
- **Active Directory Organizational Unit (OU) configuration** - Sharing an Organizational Unit (OU) between two farms or two Sites, or a farm and a Site is not supported. If you plan to configure the new Site to use Active Directory-based Controller discovery rather than the default registry-based Controller discovery, you must create a new OU to support it.
- **PortICAConfig XML file** - If you have changed the default settings for this file you may need to configure these settings for the new Site through Group Policy Objects.
- **Configuration logging settings provided through XenDesktop 4 Service Pack 1**.
- **Provisioning Services-related data**.
- **Applications**.
- **List of Controllers**.
- **NetScaler Gateway**.
- **Event log throttling settings**.

Security

Apr 04, 2016

PDF

Getting Started with Citrix XenApp and XenDesktop Security

XenApp and XenDesktop offer a secure-by-design solution that allows you to tailor your environment to your security needs.

One security concern IT faces with mobile workers is lost or stolen data. By hosting applications and desktops, XenApp and XenDesktop securely separate sensitive data and intellectual property from end-point devices by keeping all data in a data center. When policies are enabled to allow data transfer, all data is encrypted.

The XenDesktop and XenApp data centers also make incident response easier with a centralized monitoring and management service. Director allows IT to monitor and analyze data that is being accessed around the network, and Studio allows IT to patch and remedy most vulnerabilities in the data center instead of fixing the problems locally on each end-user device.

XenApp and XenDesktop also simplify audits and regulatory compliance because investigators can use a centralized audit trail to determine who accessed what applications and data. Director gathers historical data regarding updates to the system and user data usage by accessing Configuration Logging and OData API.

Delegated Administration allows you to set up administrator roles to control access to XenDesktop and XenApp at a granular level. This allows flexibility in your organization to give certain administrators full access to tasks, operations, and scopes while other administrators have limited access.

XenApp and XenDesktop give administrators granular control over users by applying policies at different levels of the network — from the local level to the Organizational Unit level. This control of policies determines if a user, device, or groups of users and devices can connect, print, copy/paste, or map local drives, which could minimize security concerns with third-party contingency workers. Administrators can also use the Desktop Lock feature so end users can only use the virtual desktop while preventing any access to the local operating system of the end-user device.

Administrators can increase security on XenApp or XenDesktop by configuring the Site to use the Secure Sockets Layer (SSL) security protocol of the Controller or between end users and Virtual Delivery Agents (VDA). Transport Layer Security (TLS) security protocol can also be enabled on a Site to provide server authentication, data stream encryption, and message integrity checks for a TCP/IP connection.

XenApp and XenDesktop also support multifactor authentication for Windows or a specific application. Multifactor authentication could also be used to manage all resources delivered by XenApp and XenDesktop. These methods include:

- Tokens
- Smart cards
- RADIUS
- Kerberos
- Biometrics

XenDesktop can be integrated with many third-party security solutions, ranging from identity management through to antivirus software. A list of supported products can be found at http://www.citrix.com/ready.

Select releases of XenApp and XenDesktop are certified for Common Criteria standard. For a list of those standards, go to

http://www.commoncriteriaportal.org/cc/.

Related content

- Security best practices and considerations
- Delegated Administration
- Smart cards
- SSL
- Desktop Lock

Security best practices and considerations

Aug 23, 2016

This document describes:

- General security best practices when using this release, and any security-related differences between this release and a conventional computer environment
- Manage user accounts
- Manage user privileges
- Manage logon rights
- Configure user rights
- Configure service settings
- Deployment scenarios and their security implications
- Remote PC Access security considerations

Your organization may need to meet specific security standards to satisfy regulatory requirements. This document does not cover this subject, because such security standards change over time. For up-to-date information on security standards and Citrix products, consult http://www.citrix.com/security/.

Security best practices

Keep all machines in your environment up to date with security patches. One advantage is that you can use thin clients as terminals, which simplifies this task.

Protect all machines in your environment with antivirus software.

Protect all machines in your environment with perimeter firewalls, including at enclave boundaries as appropriate.

If you are migrating a conventional environment to this release, you may need to reposition an existing perimeter firewall or add new perimeter firewalls. For example, suppose there is a perimeter firewall between a conventional client and database server in the data center. When this release is used, that perimeter firewall must instead be placed so that the virtual desktop and user device are on one side, and the database servers and Delivery Controllers in the data center are on the other side. You should therefore consider creating an enclave within your data center to contain the database servers and Controllers. You should also consider having protection between the user device and the virtual desktop.

All machines in your environment should be protected by a personal firewall. When you install core components and Virtual Delivery Agents (VDAs), you can choose to have the ports required for component and feature communication opened automatically if the Windows Firewall Service is detected (even if the firewall is not enabled). You can also choose to configure those firewall ports manually. If you use a different firewall, you must configure the firewall manually.

Note: TCP ports 1494 and 2598 are used for ICA and CGP and are therefore likely to be open at firewalls so that users outside the data center can access them. Citrix recommends that you do not use these ports for anything else, to avoid the possibility of inadvertently leaving administrative interfaces open to attack. Ports 1494 and 2598 are officially registered with the Internet Assigned Number Authority (see http://www.iana.org/).
All network communications should be appropriately secured and encrypted to match your security policy. You can secure all communication between Microsoft Windows computers using IPSec; refer to your operating system documentation for details about how to do this. In addition, communication between user devices and desktops is secured through Citrix SecureICA, which is configured by default to 128-bit encryption. You can configure SecureICA when you are creating or updating an assignment; see Change basic settings.

Manage user accounts

If the option to install App-V publishing components is selected when installing a Virtual Delivery Agent (VDA), or if this feature is added later, the local administrative account CtxAppVCOMAdmin is added to the VDA. If you use the App-V publishing feature, do not modify this account. If you do not need to use the App-V publishing feature, do not select it at installation time. If you later decide not to use the App-V publishing feature, you can disable or delete this account.

Manage user privileges

Grant users only the capabilities they require. Microsoft Windows privileges continue to be applied to desktops in the usual way: configure privileges through User Rights Assignment and group memberships through Group Policy. One advantage of this release is that it is possible to grant a user administrative rights to a desktop without also granting physical control over the computer on which the desktop is stored.

When planning for desktop privileges, note:

- By default, when non-privileged users connect to a desktop, they see the time zone of the system running the desktop instead of the time zone of their own user device. For information on how to allow users to see their local time when using desktops, see Change basic settings.
- A user who is an administrator on a desktop has full control over that desktop. If a desktop is a pooled desktop rather than a dedicated desktop, the user must be trusted in respect of all other users of that desktop, including future users. All users of the desktop need to be aware of the potential permanent risk to their data security posed by this situation. This consideration does not apply to dedicated desktops, which have only a single user; that user should not be an administrator on any other desktop.
- A user who is an administrator on a desktop can generally install software on that desktop, including potentially malicious software. The user can also potentially monitor or control traffic on any network connected to the desktop.

Manage logon rights

Logon rights are required for both user accounts and computer accounts. As with Microsoft Windows privileges, logon rights continue to be applied to desktops in the usual way: configure logon rights through User Rights Assignment and group memberships through Group Policy.

The Windows logon rights are: log on locally, log on through Remote Desktop Services, log on over the network (access this computer from the network), log on as a batch job, and log on as a service.

For computer accounts, grant computers only the logon rights they require. The logon right "Access this computer from the network" is required:

- At VDAs, for the computer accounts of Delivery Controllers
- At Delivery Controllers, for the computer accounts of VDAs. See Active Directory OU-based Controller discovery.
- At StoreFront servers, for the computer accounts of other servers in the same StoreFront server group

For user accounts, grant users only the logon rights they require.

According to Microsoft, by default the group Remote Desktop Users is granted the logon right "Allow log on through Remote Desktop Services" (except on domain controllers).

Your organization's security policy may state explicitly that this group should be removed from that logon right. Consider the following approach:

- The Virtual Delivery Agent (VDA) for Server OS uses Microsoft Remote Desktop Services. You can configure the Remote Desktop Users group as a restricted group, and control membership of the group via Active Directory group policies. Refer to Microsoft documentation for more information.
- For other components of XenApp and XenDesktop, including the VDA for Desktop OS, the group Remote Desktop Users is not required. So, for those components, the group Remote Desktop Users does not require the logon right "Allow log on through Remote Desktop Services"; you can remove it. Additionally:
  - If you administer those computers via Remote Desktop Services, ensure that all such administrators are already members of the Administrators group.
  - If you do not administer those computers via Remote Desktop Services, consider disabling Remote Desktop Services itself on those computers.

Although it is possible to add users and groups to the login right "Deny logon through Remote Desktop Services", the use of deny logon rights is not generally recommended. Refer to Microsoft documentation for more information.

Configure user rights

Delivery Controller installation creates the following Windows services:

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): Manages Microsoft Active Directory computer accounts for VMs.
- Citrix Analytics (NT SERVICE\CitrixAnalytics): Collects site configuration usage information for use by Citrix, if this collection been approved by the site administrator. It then submits this information to Citrix, to help improve the product.
- Citrix App Library (NT SERVICE\CitrixAppLibrary): Supports management and provisioning of AppDisks, AppDNA integration, and management of App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): Selects the virtual desktops or applications that are available to users.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): Records all configuration changes and other state changes made by administrators to the site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): Site-wide repository for shared configuration.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): Manages the permissions granted to administrators.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): Manages self-tests of the other Delivery Controller services.
- Citrix Host Service (NT SERVICE\CitrixHostService): Stores information about the hypervisor infrastructures used in a XenApp or XenDesktop deployment, and also offers functionality used by the console to enumerate resources in a hypervisor pool.
- Citrix Machine Creation Service (NT SERVICE\CitrixMachineCreationService): Orchestrates the creation of desktop VMs.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Collects metrics for XenApp or XenDesktop, stores historical information, and provides a query interface for troubleshooting and reporting tools.
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): Supports management of StoreFront. (It is not part of the StoreFront component itself.)
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): Supports privileged management operations of StoreFront. (It is not part of the StoreFront component itself.)

Delivery Controller installation also creates the following Windows services. These are also created when installed with other Citrix components:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Supports the collection of diagnostic information for use by Citrix Support.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Collects diagnostic information for analysis by Citrix, such that the analysis results and recommendations can be viewed by administrators to help diagnose issues with the site.

Except for the Citrix Storefront Privileged Administration Service, these services are granted the logon right Log on as a service and the privileges Adjust memory quotas for a process, Generate security audits, and Replace a process level token. You do not need to change these user rights. These privileges are not used by the Delivery Controller and are automatically disabled.

Configure service settings

Except for the Citrix Storefront Privileged Administration service and the Citrix Telemetry Service, the Delivery Controller Windows services listed above in the "Configure user rights" section are configured to log on as the NETWORK SERVICE identity. Do not alter these service settings.

The Citrix Storefront Privileged Administration service is configured to log on Local System (NT AUTHORITY\SYSTEM). This is required for Delivery Controller StoreFront operations that are not normally available to services (including creating Microsoft IIS sites). Do not alter its service settings.

The Citrix Telemetry Service is configured to log on as its own service-specific identity.

You can disable the Citrix Telemetry Service. Apart from this service, and services that are already disabled, do not disable any other of these Delivery Controller Windows services.

Deployment scenario security implications

Your user environment can consist either of user devices that are unmanaged by your organization and completely under the control of the user, or of user devices that are managed and administered by your organization. The security considerations for these two environments are generally different.

- **Managed user devices** - Managed user devices are under administrative control; they are either under your own control, or the control of another organization that you trust. You may configure and supply user devices directly to users; alternatively, you may provide terminals on which a single desktop runs in full-screen-only mode. You should follow the general security best practices described above for all managed user devices. This release has the advantage that minimal software is required on a user device.

  A managed user device can be set up to be used in full-screen-only mode or in window mode:

  - If a user device is configured to be used in full-screen-only mode, users log on to it with the usual Log On To Windows screen. The same user credentials are then used to log on automatically to this release.
  - If a user device is configured so that users see their desktop in a window, users first log on to the user device, then log on to this release through a Web site supplied with the release.
- **Unmanaged user devices** - User devices that are not managed and administered by a trusted organization cannot be assumed to be under administrative control. For example, you might permit users to obtain and configure their own devices, but users might not follow the general security best practices described above. This release has the advantage

that it is possible to deliver desktops securely to unmanaged user devices. These devices should still have basic antivirus protection that will defeat keylogger and similar input attacks.

- **Data storage considerations** - When using this release, you can prevent users from storing data on user devices that are under their physical control. However, you must still consider the implications of users storing data on desktops. It is not good practice for users to store data on desktops; data should be held on file servers, database servers, or other repositories where it can be appropriately protected.

  Your desktop environment may consist of various types of desktops, such as pooled and dedicated desktops:

  - Users should never store data on desktops that are shared amongst users, such as pooled desktops.
  - If users store data on dedicated desktops, that data should be removed if the desktop is later made available to other users.
- **Mixed-version environments** Mixed-version environments are inevitable during some upgrades. Follow best-practice and minimize the time that Citrix components of different versions co-exist.

  In mixed-version environments security policy, for example, may not be uniformly enforced.

  Note: This is typical of other software products; the use of an earlier version of Active Directory only partially enforces Group Policy with later versions of Windows.

  The following scenario describes a security issue that can occur in a specific mixed-version Citrix environment. When Citrix Receiver 1.7 is used to connect to a virtual desktop running the Virtual Delivery Agent in XenApp and XenDesktop 7.6 Feature Pack 2, the policy "Allow file transfer between desktop and client" is enabled in the Site but cannot be disabled by a Delivery Controller running XenApp and XenDesktop 7.1. It does not recognize the policy, which was released only in the later version of the product. This policy allows users to upload and download files to their virtual desktop – the security issue. To work around this, upgrade the Delivery Controller, or a standalone instance of Studio, to Version 7.6 Feature Pack 2 and then use GP to disable the policy. Alternatively, use local policy on all affected virtual desktops.

Remote PC Access

Remote PC Access implements the following security features:

- Smart card use is supported.
- When a remote session connects, the office PC's monitor appears as blank.
- Remote PC Access redirects all keyboard and mouse input to the remote session, except CTRL+ALT+DEL and USB-enabled smart cards and biometric devices.
- SmoothRoaming is supported for a single user only.
- When a user has a remote session connected to an office PC, only that user can resume local access of the office PC. To resume local access, the user presses Ctrl-Alt-Del on the local PC and then logs on with the same credentials used by the remote session. The user can also resume local access by inserting a smart card or leveraging biometrics, if your system has appropriate third-party Credential Provider integration.
  This default behavior can be overridden by enabling Fast User Switching via Group Policy Objects (GPOs) or by editing the registry.

- By default, Remote PC Access supports automatic assignment of multiple users to a VDA. In XenDesktop 5.6 Feature Pack 1, administrators could override this behavior using the RemotePCAccess.ps1 PowerShell script. This release uses a registry entry to allow or prohibit multiple automatic remote PC assignments; this setting applies to the entire Site.
  Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

To restrict automatic assignments to a single user:

1. Set the following registry entry on each Controller in the Site:
   HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

   Name: AllowMultipleRemotePCAssignments

   Type: REG_DWORD

   Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple user assignment.

2. If there are any existing user assignments, remove them using SDK commands for the VDA to subsequently be eligible for a single automatic assignment.
   1. Remove all assigned users from the VDA: $machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine
   2. Remove the VDA from the Delivery Group: $machine | Remove-BrokerMachine -DesktopGroup $desktopGroup
3. Restart the physical office PC.

Delegated Administration

Sep 09, 2015

The Delegated Administration model offers the flexibility to match how your organization wants to delegate administration activities, using role and object-based control. Delegated Administration accommodates deployments of all sizes, and allows you to configure more permission granularity as your deployment grows in complexity. Delegated Administration uses three concepts: administrators, roles, and scopes.

- **Administrators** — An administrator represents an individual person or a group of people identified by their Active Directory account. Each administrator is associated with one or more role and scope pairs.
- **Roles** — A role represents a job function, and has defined permissions associated with it. For example, the Delivery Group Administrator role has permissions such as 'Create Delivery Group' and 'Remove Desktop from Delivery Group.' An administrator can have multiple roles for a Site, so a person could be a Delivery Group Administrator and a Machine Catalog Administrator. Roles can be built-in or custom.
  The built-in roles are:

Role	Permissions
Full Administrator	Can perform all tasks and operations. A Full Administrator is always combined with the All scope.
Read Only Administrator	Can see all objects in specified scopes as well as global information, but cannot change anything. For example, a Read Only Administrator with Scope=London can see all global objects (such as Configuration Logging) and any London-scoped objects (for example, London Delivery Groups). However, that administrator cannot see objects in the New York scope (assuming that the London and New York scopes do not overlap).
Help Desk Administrator	Can view Delivery Groups, and manage the sessions and machines associated with those groups. Can see the Machine Catalog and host information for the Delivery Groups being monitored, and can also perform session management and machine power management operations for the machines in those Delivery Groups.
Machine Catalog Administrator	Can create and manage Machine Catalogs and provision the machines into them. Can build Machine Catalogs from the virtualization infrastructure, Provisioning Services, and physical machines. This role can manage base images and install software, but cannot assign applications or desktops to users.
Delivery Group Administrator	Can deliver applications, desktops, and machines; can also manage the associated sessions. Can also manage application and desktop configurations such as policies and power management settings.
Host Administrator	Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to users.

  In certain product editions, you can create custom roles to match the requirements of your organization, and delegate permissions with more detail. You can use custom roles to allocate permissions at the granularity of an action or task in a console.

- **Scopes** — A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to your

organization (for example, the set of Delivery Groups used by the Sales team). Objects can be in more than one scope; you can think of objects being labeled with one or more scopes. There is one built-in scope: 'All,' which contains all objects. The Full Administrator role is always paired with the All scope.

Example

Company XYZ decided to manage applications and desktops based on their department (Accounts, Sales, and Warehouse) and their desktop operating system (Windows 7 or Windows 8). The administrator created five scopes, then labeled each Delivery Group with two scopes: one for the department where they are used and one for the operating system they use.

The following administrators were created:

Administrator	Roles	Scopes
domain/fred	Full Administrator	All (the Full Administrator role always has the All scope)
domain/rob	Read Only Administrator	All
domain/heidi	Read Only Administrator Help Desk Administrator	All Sales
domain/warehouseadmin	Help Desk Administrator	Warehouse
domain/peter	Delivery Group Administrator Machine Catalog Administrator	Win7

- Fred is a Full Administrator and can view, edit, and delete all objects in the system.
- Rob can view all objects in the Site but cannot edit or delete them.
- Heidi can view all objects and can perform help desk tasks on Delivery Groups in the Sales scope. This allows her to manage the sessions and machines associated with those groups; she cannot make changes to the Delivery Group, such as adding or removing machines.
- Anyone who is a member of the warehouseadmin Active Directory security group can view and perform help desk tasks on machines in the Warehouse scope.
- Peter is a Windows 7 specialist and can manage all Windows 7 Machine Catalogs and can deliver Windows 7 applications, desktops, and machines, regardless of which department scope they are in. The administrator considered making Peter a Full Administrator for the Win7 scope; however, she decided against this, because a Full Administrator also has full rights over all objects that are not scoped, such as 'Site' and 'Administrator.'

How to use Delegated Administration

Generally, the number of administrators and the granularity of their permissions depends on the size and complexity of the deployment.

- In small or proof-of-concept deployments, one or a few administrators do everything; there is no delegation. In this case, create each administrator with the built-in Full Administrator role, which has the All scope.
- In larger deployments with more machines, applications, and desktops, more delegation is needed. Several administrators

might have more specific functional responsibilities (roles). For example, two are Full Administrators, and others are Help Desk Administrators. Additionally, an administrator might manage only certain groups of objects (scopes), such as machine catalogs. In this case, create new scopes, plus administrators with one of the built-in roles and the appropriate scopes.
- Even larger deployments might require more (or more specific) scopes, plus different administrators with unconventional roles. In this case, edit or create additional scopes, create custom roles, and create each administrator with a built-in or custom role, plus existing and new scopes.

For flexibility and ease of configuration, you can create new scopes when you create an administrator. You can also specify scopes when creating or editing Machine Catalogs or connections.

Create and manage administrators

When you create a Site as a local administrator, your user account automatically becomes a Full Administrator with full permissions over all objects. After a Site is created, local administrators have no special privileges.

The Full Administrator role always has the All scope; you cannot change this.

By default, an administrator is enabled. Disabling an administrator might be necessary if you are creating the new administrator now, but that person will not begin administration duties until later. For existing enabled administrators, you might want to disable several of them while you are reorganizing your object/scopes, then re-enable them when you are ready to go live with the updated configuration. You cannot disable a Full Administrator if it will result in there being no enabled Full Administrator. The enable/disable check box is available when you create, copy, or edit an administrator.

When you delete a role/scope pair while copying, editing, or deleting an administrator, it deletes only the relationship between the role and the scope for that administrator; it does not delete either the role or the scope, nor does it affect any other administrator who is configured with that role/scope pair.

To manage administrators, click Configuration > Administrators in the Studio navigation pane, and then click the Administrators tab in the upper middle pane.
- To create an administrator, click Create new Administrator in the Actions pane. Type or browse to the user account name, select or create a scope, and select a role. The new administrator is enabled by default; you can change this.
- To copy an administrator, select the administrator in the middle pane and then click Copy Administrator in the Actions pane. Type or browse to the user account name. You can select and then edit or delete any of the role/scope pairs, and add new ones. The new administrator is enabled by default; you can change this.
- To edit an administrator, select the administrator in the middle pane and then click Edit Administrator in the Actions pane. You can edit or delete any of the role/scope pairs, and add new ones.
- To delete an administrator, select the administrator in the middle pane and then click Delete Administrator in the Actions pane. You cannot delete a Full Administrator if it will result in there being no enabled Full Administrator.

Create and manage roles

Role names can contain up to 64 Unicode characters; they cannot contain the following characters: \ (backslash), / (forward slash), ; (semicolon), : (colon), # (pound sign) , (comma), * (asterisk), ? (question mark), = (equal sign), < (left arrow), > (right arrow), | (pipe), [ ] (left or right bracket), ( ) (left or right parenthesis), " (quotation marks), and ' (apostrophe). Descriptions can contain up to 256 Unicode characters.

You cannot edit or delete a built-in role. You cannot delete a custom role if any administrator is using it.

Note: Only certain product editions support custom roles. Editions that do not support custom roles do not have related entries in the Actions pane.

To manage roles, click Configuration > Administrators in the Studio navigation pane, and then click the Roles tab in the upper middle pane.

- To view role details, select the role in the middle pane. The lower portion of the middle pane lists the object types and associated permissions for the role. Click the Administrators tab in the lower pane to display a list of administrators who currently have this role.
- To create a custom role, click Create new Role in the Actions pane. Enter a name and description. Select the object types and permissions.
- To copy a role, select the role in the middle pane and then click Copy Role in the Actions pane. Change the name, description, object types, and permissions, as needed.
- To edit a custom role, select the role in the middle pane and then click Edit Role in the Actions pane. Change the name, description, object types, and permissions, as needed.
- To delete a custom role, select the role in the middle pane and then click Delete Role in the Actions pane. When prompted, confirm the deletion.

Create and manage scopes

When you create a Site, the only available scope is the 'All' scope, which cannot be deleted.

You can create scopes using the procedure below. You can also create scopes when you create an administrator; each administrator must be associated with at least one role and scope pair. When you are creating or editing desktops, machine catalogs, applications, or hosts, you can add them to an existing scope; if you do not add them to a scope, they remain part of the 'All' scope.

Site creation cannot be scoped, nor can Delegated Administration objects (scopes and roles). However, objects you cannot scope are included in the 'All' scope. (Full Administrators always have the All scope.) Machines, power actions, desktops, and sessions are not directly scoped; administrators can be allocated permissions over these objects through the associated machine catalogs or Delivery Groups.

Scope names can contain up to 64 Unicode characters; they cannot include the following characters: \ (backslash), / (forward slash), ; (semicolon), : (colon), # (pound sign) , (comma), * (asterisk), ? (question mark), = (equal sign), < (left arrow), > (right arrow), | (pipe), [ ] (left or right bracket), ( ) (left or right parenthesis), " (quotation marks), and ' (apostrophe). Descriptions can contain up to 256 Unicode characters.

When you copy or edit a scope, keep in mind that removing objects from the scope can make those objects inaccessible to the administrator. If the edited scope is paired with one or more roles, ensure that the scope updates you make do not make any role/scope pair unusable.

To manage scopes, click Configuration > Administrators in the Studio navigation pane, and then click the Scopes tab in the upper middle pane.

- To create a scope, click Create new Scope in the Actions pane. Enter a name and description. To include all objects of a particular type (for example, Delivery Groups), select the object type. To include specific objects, expand the type and then select individual objects (for example, Delivery Groups used by the Sales team).
- To copy a scope, select the scope in the middle pane and then click Copy Scope in the Actions pane. Enter a name and description. Change the object types and objects, as needed.
- To edit a scope, select the scope in the middle pane and then click Edit Scope in the Actions pane. Change the name, description, object types, and objects, as needed.
- To delete a scope, select the scope in the middle pane and then click Delete Scope in the Actions pane. When prompted, confirm the deletion.

Create reports

You can create two types of Delegated Administration reports:

- An HTML report that lists the role/scope pairs associated with an administrator, plus the individual permissions for each type of object (for example, Delivery Groups and Machine Catalogs). You generate this report from Studio.
  To create this report, click Configuration > Administrators in the navigation pane. Select an administrator in the middle pane and then click Create Report in the Actions pane.

  You can also request this report when creating, copying, or editing an administrator.

- An HTML or CSV report that maps all built-in and custom roles to permissions. You generate this report by running a PowerShell script named OutputPermissionMapping.ps1.
  To run this script, you must be a Full Administrator, a Read Only Administrator, or a custom administrator with permission to read roles. The script is located in: Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\.

  Syntax:

  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path <string>] [-AdminAddress <string>] [-Show] [<CommonParameters>]

Parameter	Description
-Help	Displays script help.
-Csv	Specifies CSV output. Default = HTML
-Path <string>	Where to write the output. Default = stdout
-AdminAddress <string>	IP address or host name of the Delivery Controller to connect to. Default = localhost
-Show	(Valid only when the -Path parameter is also specified) When you write the output to a file, -Show causes the output to be opened in an appropriate program, such as a web browser.
<CommonParameters>	Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, and OutVariable. For details, see the Microsoft documentation.

The following example writes an HTML table to a file named Roles.html and opens the table in a web browser.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html –Show
```

The following example writes a CSV table to a file named Roles.csv. The table is not displayed.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
–CSV -Path Roles.csv
```

From a Windows command prompt, the preceding example command is:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
```

```
-CSV -Path Roles.csv"
```

Smart cards

Aug 29, 2016

Smart cards and equivalent technologies are supported within the guidelines described in this article. To use smart cards with XenApp or XenDesktop:

- Understand your organization's security policy concerning the use of smart cards. These policies might, for example, state how smart cards are issued and how users should safeguard them. Some aspects of these policies might need to be reassessed in a XenApp or XenDesktop environment.
- Determine which user device types, operating systems, and published applications are to be used with smart cards.
- Familiarize yourself with smart card technology and your selected smart card vendor hardware and software.
- Know how to deploy digital certificates in a distributed environment.

Types of smart cards

Enterprise and consumer smart cards have the same dimensions, electrical connectors, and fit the same smart card readers.

Smart cards for enterprise use contain digital certificates. These smart cards support Windows logon, and can also be used with applications for digital signing and encryption of documents and e-mail. XenApp and XenDesktop support these uses.

Smart cards for consumer use do not contain digital certificates; they contain a shared secret. These smart cards can support payments (such as a chip-and-signature or chip-and-PIN credit card). They do not support Windows logon or typical Windows applications. Specialized Windows applications and a suitable software infrastructure (including, for example, a connection to a payment card network) are needed for use with these smart cards. Contact your Citrix representative for information on supporting these specialized applications on XenApp or XenDesktop.

For enterprise smart cards, there are compatible equivalents that can be used in a similar way.

- A smart card-equivalent USB token connects directly to a USB port. These USB tokens are usually the size of a USB flash drive, but can be as small as a SIM card used in a mobile phone. They appear as the combination of a smart card plus a USB smart card reader.
- A virtual smart card using a Windows Trusted Platform Module (TPM) appears as a smart card. These virtual smart cards are supported for Windows 8 and Windows 10, using Citrix Receiver minimum 4.3.
  - Versions of XenApp and XenDesktop earlier than 7.6 FP3 do not support virtual smart cards.
  - For more information on virtual smart cards, see Virtual Smart Card Overview.

    Note: The term "virtual smart card" is also used to describe a digital certificate simply stored on the user computer. These digital certificates are not strictly equivalent to smart cards.

XenApp and XenDesktop smart card support is based on the Microsoft Personal Computer/Smart Card (PC/SC) standard specifications. A minimum requirement is that smart cards and smart card devices must be supported by the underlying Windows operating system and must be approved by the Microsoft Windows Hardware Quality Labs (WHQL) to be used on computers running qualifying Windows operating systems. See the Microsoft documentation for additional information about hardware PC/SC compliance. Other types of user devices may comply with the PS/SC standard. For more information, refer to the Citrix Ready program at http://www.citrix.com/ready/.

Usually, a separate device driver is needed for each vendor's smart card or equivalent. However, if smart cards conform to a

standard such as the NIST Personal Identity Verification (PIV) standard, it may be possible to use a single device driver for a range of smart cards. The device driver must be installed on both the user device and the Virtual Delivery Agent (VDA). The device driver is often supplied as part of a smart card middleware package available from a Citrix partner; the smart card middleware package will offer advanced features. The device driver may also be described as a Cryptographic Service Provider (CSP), Key Storage Provider (KSP), or minidriver.

The following smart card and middleware combinations for Windows systems have been tested by Citrix as representative examples of their type. However, other smart cards and middleware can also be used. For more information about Citrix-compatible smart cards and middleware, see http://www.citrix.com/ready.

Middleware	Matching cards
ActivClient 7.0 (DoD mode enabled)	DoD CAC card
ActivClient 7.0 in PIV mode	NIST PIV card
Microsoft mini driver	NIST PIV card
GemAlto Mini Driver for .NET card	GemAlto .NET v2+
Microsoft native driver	Virtual Smart Cards (TPM)

For information about smart card usage with other types of devices, see the Citrix Receiver documentation for that device.For more information about PIV usage with XenDesktop, see Configuring Citrix XenDesktop 7.6 and NetScaler Gateway 10.5 with PIV Smart Card Authentication.

For information about smart card usage with other types of devices, see the Citrix Receiver documentation for that device.

Remote PC Access

Smart cards are supported only for remote access to physical office PCs running Windows 10, Windows 8 or Windows 7; smart cards are not supported for office PCs running Windows XP.

The following smart cards were tested with Remote PC Access:

Middleware	Matching cards
Gemalto .NET minidriver	Gemalto .NET v2+
ActivIdentity ActivClient 6.2	NIST PIV
ActivIdentity ActivClient 6.2	CAC
Microsoft minidriver	NIST PIV

Microsoft native driver	Virtual smart cards

Types of smart card readers

A smart card reader may be built in to the user device, or be separately attached to the user device (usually via USB or Bluetooth). Contact card readers that comply with the USB Chip/Smart Card Interface Devices (CCID) specification are supported. They contain a slot or swipe into which the user inserts the smart card. The Deutsche Kreditwirtschaft (DK) standard defines four classes of contact card readers.

- Class 1 smart card readers are the most common, and usually just contain a slot. Class 1 smart card readers are supported, usually with a standard CCID device driver supplied with the operating system.
- Class 2 smart card readers also contain a secure keypad that cannot be accessed by the user device. Class 2 smart card readers may be built into a keyboard with an integrated secure keypad. For class 2 smart card readers, contact your Citrix representative; a reader-specific device driver may be required to enable the secure keypad capability.
- Class 3 smart card readers also contain a secure display. Class 3 smart card readers are not supported.
- Class 4 smart card readers also contain a secure transaction module. Class 4 smart card readers are not supported.

Note: The smart card reader class is unrelated to the USB device class.

Smart card readers must be installed with a corresponding device driver on the user device.

User experience

Smart card support is integrated into XenApp and XenDesktop, using a specific ICA/HDX smart card virtual channel that is enabled by default.

Important: Do not use generic USB redirection for smart card readers. This is disabled by default for smart card readers, and is not supported if enabled.

Multiple smart cards and multiple readers can be used on the same user device, but if pass-through authentication is in use, only one smart card must be inserted when the user starts a virtual desktop or application. When a smart card is used within an application (for example, for digital signing or encryption functions), there might be additional prompts to insert a smart card or enter a PIN. This can occur if more than one smart card has been inserted at the same time.

- If users are prompted to insert a smart card when the smart card is already in the reader, they should select Cancel.
- If users are prompted for the PIN, they should enter the PIN again.

If you are using hosted applications running on Windows Server 2008 or 2008 R2 and with smart cards requiring the Microsoft Base Smart Card Cryptographic Service Provider, you might find that if a user runs a smart card transaction, all other users who use a smart card in the logon process are blocked. For further details and a hotfix for this issue, see http://support.microsoft.com/kb/949538.

You can reset PINs using a card management system or vendor utility.

Before deploying smart cards

- Obtain a device driver for the smart card reader and install it on the user device. Many smart card readers can use the CCID device driver supplied by Microsoft.
- Obtain a device driver and cryptographic service provider (CSP) software from your smart card vendor, and install them on both user devices and virtual desktops. The driver and CSP software must be compatible with XenApp and XenDesktop; check the vendor documentation for compatibility. For virtual desktops using smart cards that support and use the minidriver model, smart card minidrivers should download automatically, but you can obtain them from http://catalog.update.microsoft.com or from your vendor. Additionally, if PKCS#11 middleware is required, obtain it from the card vendor.
- **Important:** Citrix recommends that you install and test the drivers and CSP software on a physical computer before installing Citrix software.
- Add the Citrix Receiver for Web URL to the Trusted Sites list for users who work with smart cards in Internet Explorer with Windows 10. In Windows 10, Internet Explorer does not run in protected mode by default for trusted sites.
- Ensure that your public key infrastructure (PKI) is configured appropriately. This includes ensuring that certificate-to-account mapping is correctly configured for Active Directory environment and that user certificate validation can be performed successfully.
- Ensure your deployment meets the system requirements of the other Citrix components used with smart cards, including Citrix Receiver and StoreFront.
- Ensure access to the following servers in your Site:
  - The Active Directory domain controller for the user account that is associated with a logon certificate on the smart card
  - Delivery Controller
  - Citrix StoreFront
  - Citrix NetScaler Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Optional for Remote PC Access): Microsoft Exchange Server

Enable smart card use

Step 1. Issue smart cards to users according to your card issuance policy.

Step 2. (Optional) Set up the smart cards to enable users for Remote PC Access.

Step 3. Install and configure the Delivery Controller and StoreFront (if not already installed) for smart card remoting.

Step 4. Enable StoreFront for smart card use. For details, see Configure smart card authentication in the StoreFront documentation.

Step 5. Enable NetScaler Gateway/Access Gateway for smart card use. For details, see Configuring Authentication and Authorization and Configuring Smart Card Access with the Web Interface in the NetScaler documentation.

Step 6. Enable VDAs for smart card use.

- Ensure the VDA has the required applications and updates.
- Install the middleware.

- Set up smart card remoting, enabling the communication of smart card data between Citrix Receiver on a user device and a virtual desktop session.

Step 7. Enable user devices (including domain-joined or non-domain-joined machines) for smart card use. See Configure smart card authentication in the StoreFront documentation for details.

- Import the certificate authority root certificate and the issuing certificate authority certificate into the device's keystore.
- Install your vendor's smart card middleware.
- Install and configure Citrix Receiver for Windows, being sure to import icaclient.adm using the Group Policy Management Console and enable smart card authentication.

Step 8. Test the deployment. Ensure that the deployment is configured correctly by launching a virtual desktop with a test user's smart card. Test all possible access mechanisms (for example, accessing the desktop through Internet Explorer and Citrix Receiver).

Smart card deployments

Sep 14, 2015

The following types of smart card deployments are supported by this product version and by mixed environments containing this version. Other configurations might work but are not supported.

Type	StoreFront connectivity
Local domain-joined computers	Directly connected
Remote access from domain-joined computers	Connected through NetScaler Gateway
Non-domain-joined computers	Directly connected
Remote access from non-domain-joined computers	Connected through NetScaler Gateway
Non-domain-joined computers and thin clients accessing the Desktop Appliance site	Connected through Desktop Appliance sites
Domain-joined computers and thin clients accessing StoreFront through the XenApp Services URL	Connected through XenApp Services URLs

The deployment types are defined by the characteristics of the user device to which the smart card reader is connected:

- Whether the device is domain-joined or non-domain-joined.
- How the device is connected to StoreFront.
- What software is used to view virtual desktops and applications.

In addition, smart card-enabled applications such as Microsoft Word, and Microsoft Excel can be used in these deployments. Those applications allow users to digitally sign or encrypt documents.

Bimodal authentication

Where possible in each of these deployments, Receiver supports bimodal authentication by offering the user a choice between using a smart card and entering their user name and password. This is useful if the smart card cannot be used (for example, the user has left it at home or the logon certificate has expired).

Because users of non-domain-joined devices log on to Receiver for Windows directly, you can enable users to fall back to explicit authentication. If you configure bimodal authentication, users are initially prompted to log on using their smart cards and PINs but have the option to select explicit authentication if they experience any issues with their smart cards.

If you deploy NetScaler Gateway, users log on to their devices and are prompted by Receiver for Windows to authenticate to NetScaler Gateway. This applies to both domain-joined and non-domain-joined devices. Users can log on to NetScaler Gateway using either their smart cards and PINs, or with explicit credentials. This enables you to provide users with bimodal authentication for NetScaler Gateway logons. Configure pass-through authentication from NetScaler Gateway to StoreFront and delegate credential validation to NetScaler Gateway for smart card users so that users are silently

authenticated to StoreFront.

Multiple Active Directory forest considerations

In a Citrix environment, smart cards are supported within a single forest. Smart card logons across forests require a direct two-way forest trust to all user accounts. More complex multi-forest deployments involving smart cards (that is, where trusts are only one-way or of different types) are not supported.

You can use smart cards in a Citrix environment that includes remote desktops. This feature can be installed locally (on the user device that the smart card is connected to) or remotely (on the remote desktop that the user device connects to).

Smart card removal policy

The smart card removal policy set on the product determines what happens if you remove the smart card from the reader during a session. The smart card removal policy is configured through and handled by the Windows operating system.

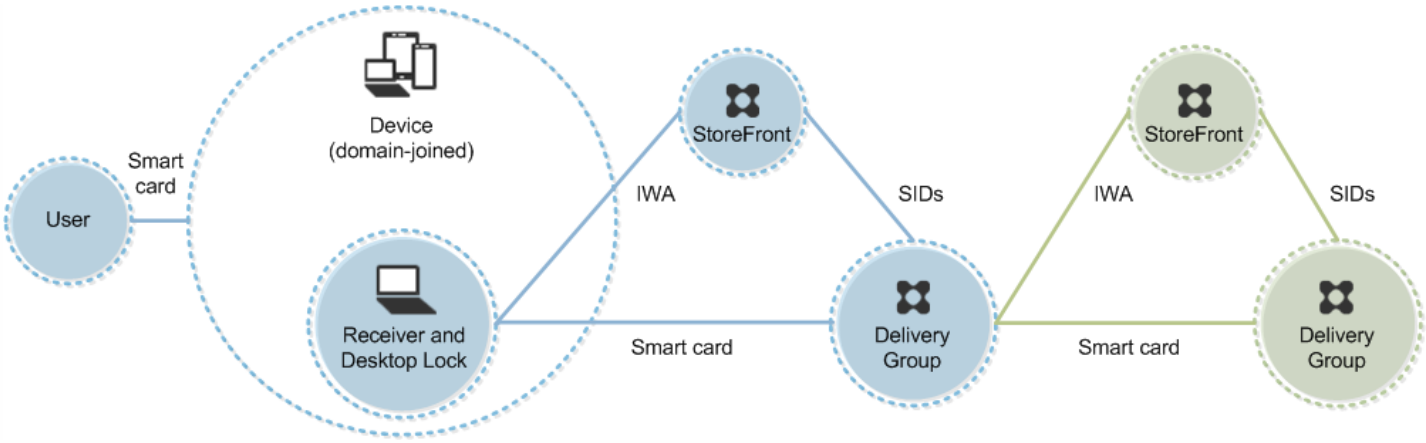
Policy setting	Desktop behavior
No action	No action.
Lock workstation	The desktop session is disconnected and the virtual desktop is locked.
Force logoff	The user is forced to log off. If the network connection is lost and this setting is enabled, the session may be logged off and the user may lose data.
Disconnect if a remote Terminal Services session	The session is disconnected and the virtual desktop is locked.

Certificate revocation checking

If certificate revocation checking is enabled and a user inserts a smart card with an invalid certificate into a card reader, the user cannot authenticate or access the desktop or application related to the certificate. For example, if the invalid certificate is used for email decryption, the email remains encrypted. If other certificates on the card, such as ones used for authentication, are still valid, those functions remain active.

Deployment example: domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.

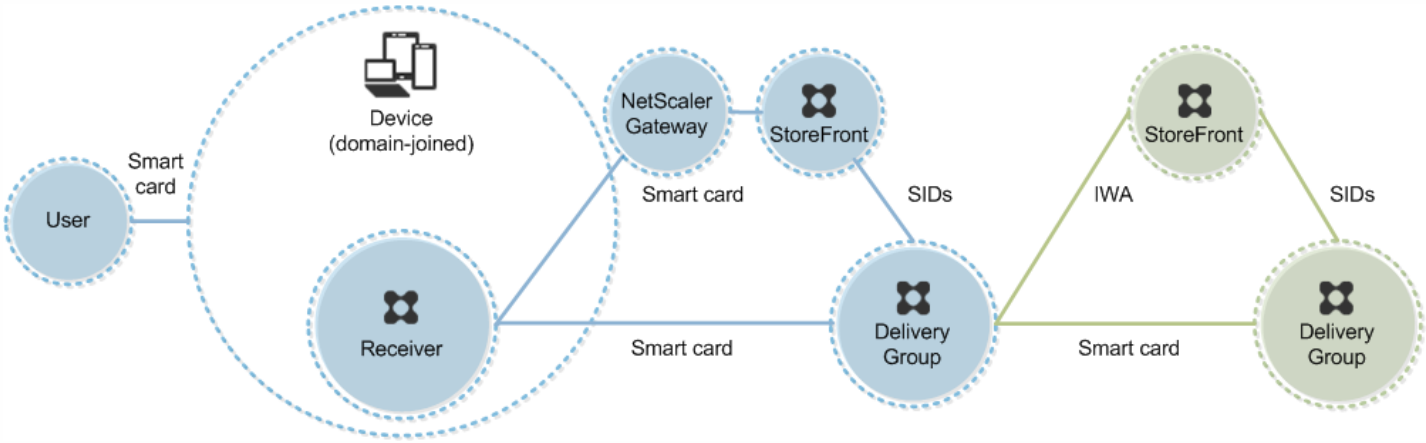


A user logs on to a device using a smart card and PIN. Receiver authenticates the user to a Storefront server using Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is not prompted for a PIN again because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: remote access from domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect to StoreFront through NetScaler Gateway/Access Gateway.



A user logs on to a device using a smart card and PIN, and then logs on again to NetScaler Gateway/Access Gateway. This second logon can be with either the smart card and PIN or a user name and password because Receiver allows bimodal authentication in this deployment.

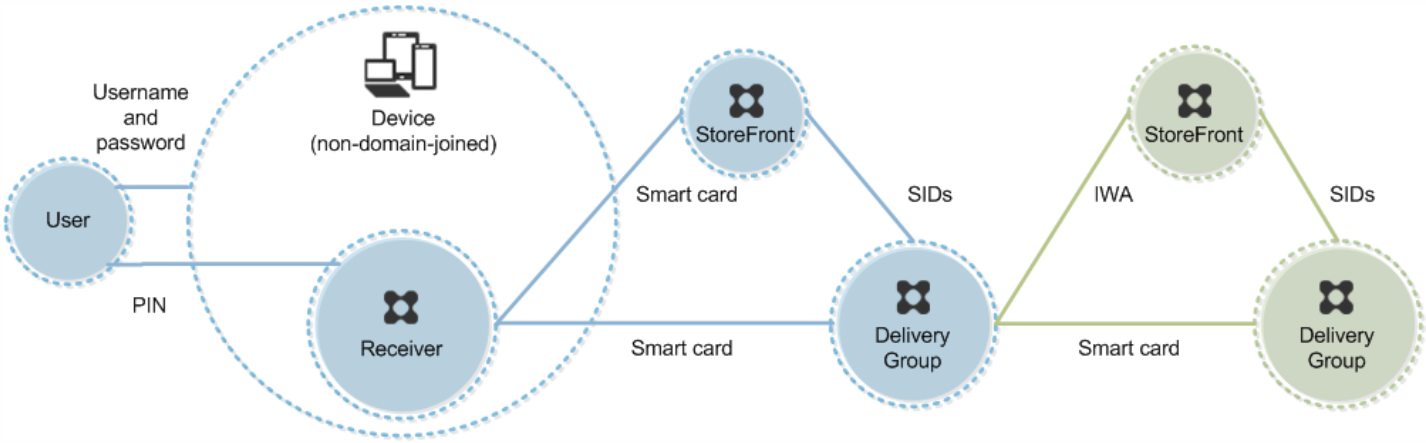
The user is automatically logged on to StoreFront, which passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is not prompted again for a PIN because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting

applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: non-domain-joined computers

This deployment involves non-domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.



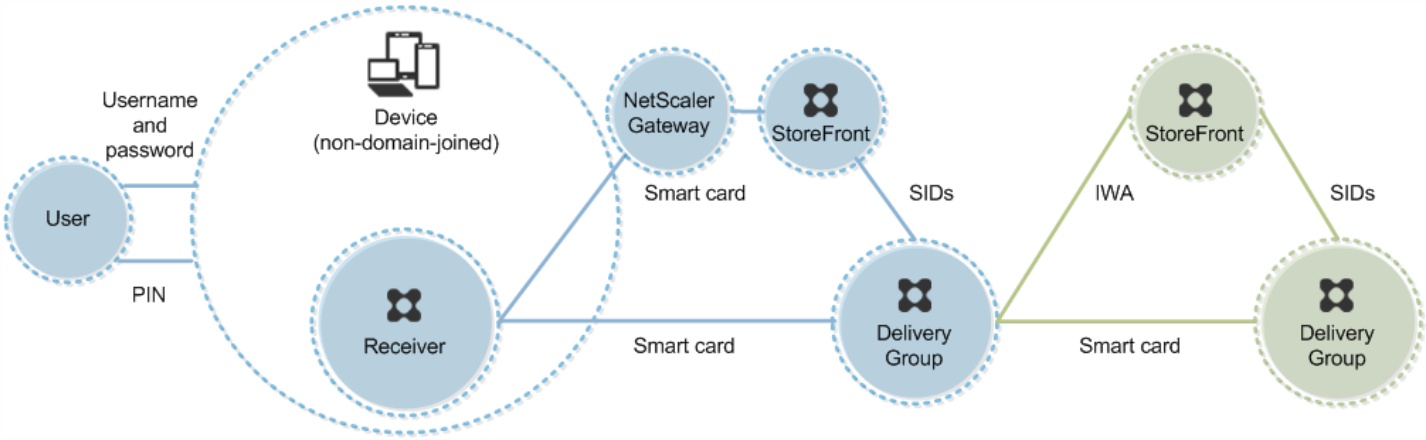
A user logs on to a device. Typically, the user enters a user name and password but, since the device is not joined to a domain, credentials for this logon are optional. Because bimodal authentication is possible in this deployment, Receiver prompts the user either for a smart card and PIN or a user name and password. Receiver then authenticates to Storefront.

StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: remote access from non-domain-joined computers

This deployment involves non-domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.



A user logs on to a device. Typically, the user enters a user name and password but, since the device is not joined to a domain, credentials for this logon are optional. Because bimodal authentication is possible in this deployment, Receiver prompts the user either for a smart card and PIN or a user name and password. Receiver then authenticates to Storefront.

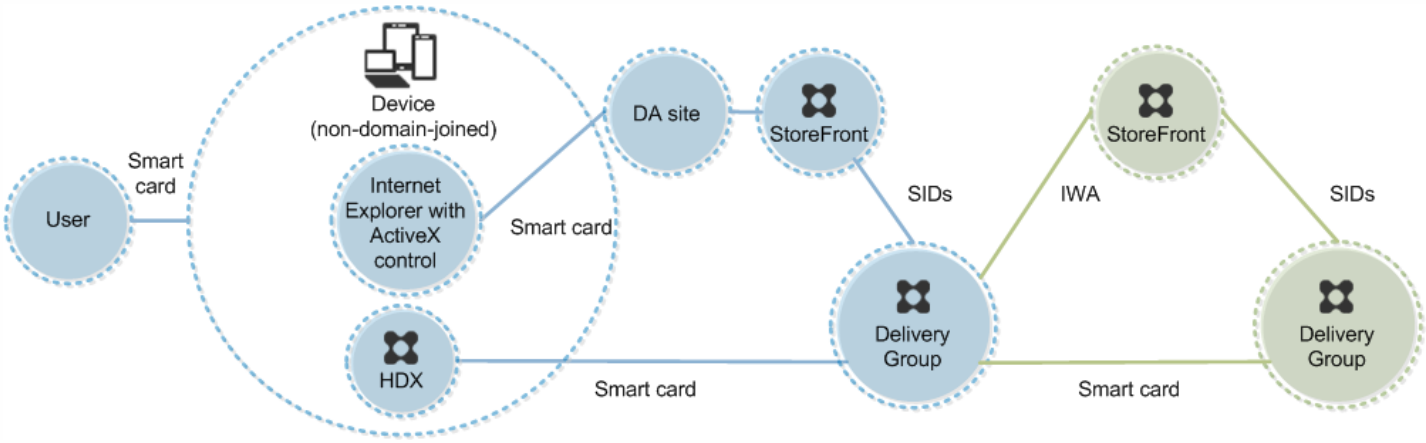
StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: non-domain-joined computers and thin clients accessing the Desktop Appliance site

This deployment involves non-domain-joined user devices that may run the Desktop Lock and connect to StoreFront through Desktop Appliance sites.

The Desktop Lock is a separate component that is released with XenApp, XenDesktop, and VDI-in-a-Box. It is an alternative to the Desktop Viewer and is designed mainly for repurposed Windows computers and Windows thin clients. The Desktop Lock replaces the Windows shell and Task Manager in these user devices, preventing users from accessing the underlying devices. With the Desktop Lock, users can access Windows Server Machine desktops and Windows Desktop Machine desktops. Installation of Desktop Lock is optional.



A user logs on to a device with a smart card. If Desktop Lock is running on the device, the device is configured to launch a Desktop Appliance site through Internet Explorer running in Kiosk Mode. An ActiveX control on the site prompts the user for a PIN, and sends it to StoreFront. StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. The first available desktop in the alphabetical list in an assigned Desktop Group starts.

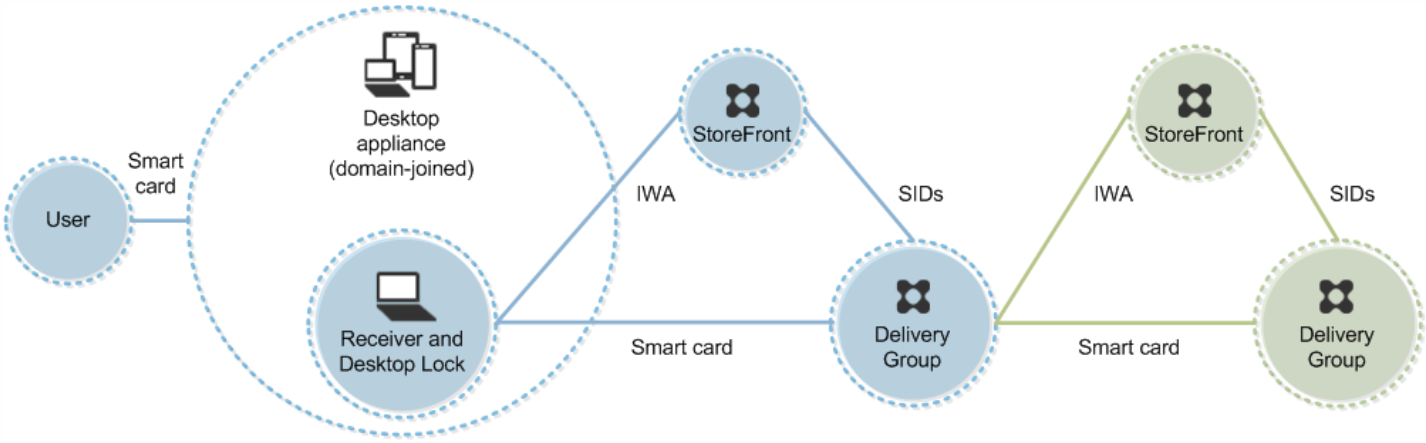
This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: domain-joined computers and thin clients accessing StoreFront through the XenApp Services URL

This deployment involves domain-joined user devices that run the Desktop Lock and connect to StoreFront through

XenApp Services URLs.

The Desktop Lock is a separate component that is released with XenApp, XenDesktop, and VDI-in-a-Box. It is an alternative to the Desktop Viewer and is designed mainly for repurposed Windows computers and Windows thin clients. The Desktop Lock replaces the Windows shell and Task Manager in these user devices, preventing users from accessing the underlying devices. With the Desktop Lock, users can access Windows Server Machine desktops and Windows Desktop Machine desktops. Installation of Desktop Lock is optional.



A user logs on to a device using a smart card and PIN. If Desktop Lock is running on the device, it authenticates the user to a Storefront server using Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop, the user is not prompted for a PIN again because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Pass-through authentication and single sign-on with smart cards

Oct 16, 2015

Pass-through authentication

Pass-through authentication with smart cards to virtual desktops is supported on user devices running Windows 10, and Windows 8 and Windows 7 SP1 Enterprise and Professional Editions.

Pass-through authentication with smart cards to hosted applications is supported on servers running Windows Server 2008 and Windows Server 2012.

To use pass-through authentication with smart cards hosted applications, ensure you enable the use of Kerberos when you configure Pass-through with smartcard as the authentication method for the site.

Note: The availability of pass-through authentication with smart cards depends on many factors including, but not limited to:

- Your organization's security policies regarding pass-through authentication.
- Middleware type and configuration.
- Smart card reader types.
- Middleware PIN caching policy.

Pass-through authentication with smart cards is configured on Citrix StoreFront. See *— Configure the authentication service* in the StoreFront documentation for details.

Single sign-on

Single sign-on is a Citrix feature that implements pass-through authentication with virtual desktop and application launches. You can use this feature in domain-joined, direct-to-StoreFront and domain-joined, NetScaler-to-StoreFront smart card deployments to reduce the number of times that users enter their PIN. To use single sign-on in these deployment types, edit the following parameters in the default.ica file, which is located on the StoreFront server:

- Domain-joined, direct-to-StoreFront smart card deployments — Set DisableCtrlAltDel to Off
- Domain-joined, NetScaler-to-StoreFront smart card deployments — Set UseLocalUserAndPassword to On

For more instructions on setting these parameters, see the StoreFront or NetScaler Gateway documentation.

The availability of single sign-on functionality depends on many factors including, but not limited to:

- Your organization's security policies regarding single sign-on.
- Middleware type and configuration.
- Smart card reader types.
- Middleware PIN caching policy.

Note: When the user logs on to the Virtual Delivery Agent (VDA) on a machine with an attached smart card reader, a Windows tile may appear representing the previous successful mode of authentication, such as smart card or password. As a result, when single sign-on is enabled, the single sign-on tile may appear. To log on, the user must select Switch Users to select another tile because the single sign-on tile will not work.

SSL

May 18, 2016

Configuring a XenApp or XenDesktop Site to use the Secure Sockets Layer (SSL) security protocol includes the following procedures:

- Obtain, install, and register a server certificate on all Delivery Controllers, and configure a port with the SSL certificate. For details, see Install SSL server certificates on Controllers.
  Optionally, you can change the ports the Controller uses to listen for HTTP and HTTPS traffic.

- Enable SSL connections between users and Virtual Delivery Agents (VDAs) by completing the following tasks:
  - Configure SSL on the machines where the VDAs are installed. (For convenience, further references to machines where VDAs are installed are simply called "VDAs.") You can use a PowerShell script supplied by Citrix, or configure it manually. For general information, see About SSL settings on VDAs. For details, see Configure SSL on a VDA using the PowerShell script and Manually configure SSL on a VDA.
  - Configure SSL in the Delivery Groups containing the VDAs by running a set of PowerShell cmdlets in Studio. For details, see Configure SSL on Delivery Groups.

  Requirements and considerations:
  - Enabling SSL connections between users and VDAs is valid only for XenApp 7.6 and XenDesktop 7.6 Sites, plus later supported releases.
  - Configure SSL in the Delivery Groups and on the VDAs after you install components, create a Site, create Machine Catalogs, and create Delivery Groups.
  - To configure SSL in the Delivery Groups, you must have permission to change Controller access rules; a Full Administrator has this permission.
  - To configure SSL on the VDAs, you must be a Windows administrator on the machine where the VDA is installed.
  - If you intend to configure SSL on VDAs that have been upgraded from earlier versions, uninstall any SSL relay software on those machines before upgrading them.
  - The PowerShell script configures SSL on static VDAs; it does not configure SSL on pooled VDAs that are provisioned by Machine Creation Services or Provisioning Services, where the machine image resets on each restart.

For tasks that include working in the Windows registry:
Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.
For information about enabling SSL to the Site database, see CTX137556.

Install SSL server certificates on Controllers

For HTTPS, the XML Service supports SSL features through the use of server certificates, not client certificates. To obtain, install, and register a certificate on a Controller, and to configure a port with the SSL certificate:

- If the Controller has IIS installed, follow the guidance in https://technet.microsoft.com/en-us/library/cc771438%28v=ws.10%29.aspx.
- If the Controller does not have IIS installed, one method of configuring the certificate is:
  1. Obtain an SSL server certificate and install it on the Controller using the guidance in http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx. For information on the certreq tool, see http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx.
     If you intend to use the PowerShell script to configure SSL on VDAs, and unless you intend on specifying the SSL certificate's thumbprint, make sure the certificate is located in the Local Computer > Personal > Certificates area of

the certificate store. If more than one certificate resides in that location, the first one found will be used.

2. Configure a port with the certificate; see http://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx.

Change HTTP or HTTPS ports

By default, the XML Service on the Controller listens on port 80 for HTTP traffic and port 443 for HTTPS traffic. Although you can use non-default ports, be aware of the security risks of exposing a Controller to untrusted networks. Deploying a standalone StoreFront server is preferable to changing the defaults.
To change the default HTTP or HTTPS ports used by the Controller, run the following command from Studio:
BrokerService.exe -WIPORT <http-port> -WISSLPORT <https-port>

where <http-port> is the port number for HTTP traffic and <https-port> is the port number for HTTPS traffic.

Note: After changing a port, Studio might display a message about license compatibility and upgrading. To resolve the issue, re-register service instances using the following PowerShell cmdlet sequence:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
XML_HTTPS | Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
Register-ConfigServiceInstance
```

Enforce HTTPS traffic only

If you want the XML Service to ignore HTTP traffic, set the following registry value in HKLM\Software\Citrix\DesktopServer\ on the Controller and then restart the Broker Service.

To ignore HTTP traffic, set XmlServicesEnableNonSsl to 0.

There is a corresponding registry value to ignore HTTPS traffic: XmlServicesEnableSsl. Ensure that this is not set to 0.

About SSL settings on VDAs

When you configure SSL on VDAs, it changes permissions on the installed SSL certificate, giving the ICA Service read access to the certificate's private key, and informing the ICA Service of the following:

- **Which certificate in the certificate store to use for SSL**.
- **Which TCP port number to use for SSL connections**.
  The Windows Firewall (if it is enabled) must be configured to allow incoming connection on this TCP port. This configuration is done for you when you use the PowerShell script.

- **Which versions of the SSL protocol to allow**.
  The supported SSL protocol versions follow a hierarchy (lowest to highest): SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. You specify the minimum allowed version; all protocol connections using that version or a higher version are allowed.

  For example, if you specify TLS 1.1 as the minimum version, then TLS 1.1 and TLS 1.2 protocol connections are allowed. If you specify SSL 3.0 as the minimum version, then connections for all the supported versions are allowed. If you specify TLS 1.2 as the minimum version, only TLS 1.2 connections are allowed.

- **Which SSL ciphers to allow**.
  A cipher suite is a list of common SSL ciphers. When a client connects and sends a list of supported SSL ciphers, the VDA matches one of the client's ciphers with one of the ciphers in its configured cipher suite and accepts the connection. If the client sends a cipher that is not in the VDA's cipher suite, the VDA rejects the connection.

Three cipher suites are supported: GOV(ernment), COM(mercial), and ALL. The ciphers in those cipher suites depend on the Windows FIPS mode; see http://support.microsoft.com/kb/811833 for information about Windows FIPS mode. The following table lists the ciphers in each supported cipher suite.

SSL cipher suite	GOV	COM	ALL	GOV	COM	ALL
FIPS Mode	Off	Off	Off	On	On	On
RSA_KEYX	x	x	x	x	x	x
RSA_SIGN	x	x	x	x	x	x
3DES	x		x	x		x
RC4		x	x			
MD5	x	x	x			
SHA	x	x	x	x	x	x
SHA_256	x	x	x	x	x	x
SHA_384	x	x	x	x	x	x
SHA_512	x	x	x	x	x	x
AES	x	x	x	x	x	x

A Delivery Group cannot have a mixture of some VDAs with SSL configured and some VDAs without SSL configured. When you configure SSL for a Delivery Group, you should have already configured SSL for all of the VDAs in that Delivery Group.

Configure SSL on a VDA using the PowerShell script

The Enable-VdaSSL.ps1 script enables or disables the SSL listener on a VDA. This script is available in the Support >Tools > SslSupport folder on the installation media.

When you enable SSL, the script disables all existing Windows Firewall rules for the specified TCP port before adding a new rule that allows the ICA Service to accept incoming connections only on the SSL TCP port. It also disables the Windows Firewall rules for:

- Citrix ICA (default: 1494)
- Citrix CGP (default: 2598)
- Citrix WebSocket (default: 8008)

The result is that users can connect only over SSL; they cannot use raw ICA, CGP, or WebSocket to connect.

The script contains the following syntax descriptions, plus additional examples; you can use a tool such as Notepad++ to review this information.

You must specify either the –Enable or –Disable parameter; all other parameters are optional.

Syntax

Enable-VdaSSL {-Enable | -Disable} [–SSLPort <port>] [-SSLMinVersion “<min-ssl-version>”] [-SSLCipherSuite “<suite>”] [-CertificateThumbPrint “<thumbprint>”]

Parameter	Description
-Enable	Installs and enables the SSL listener on the VDA. Either this parameter or the –Disable parameter is required.
-Disable	Disables the SSL listener on the VDA. Either this parameter or the –Enable parameter is required. If you specify this parameter, no other parameters are valid.
–SSLPort <port>	SSL port. Default: 443
-SSLMinVersion “<min-ssl-version>”	Minimum SSL protocol version, enclosed in quotation marks. Valid values: "SSL_3.0", "TLS_1.0", "TLS_1.1", and "TLS_1.2". Default: "TLS_1.0"
-SSLCipherSuite “<suite>”	SSL cipher suite, enclosed in quotation marks. Valid values: "GOV", "COM", and "ALL". Default: "ALL"
-CertificateThumbPrint “<thumbprint>”	Thumbprint of the SSL certificate in the certificate store, enclosed in quotation marks. This parameter is generally used when the certificate store has multiple certificates; the script uses the thumbprint to select the certificate you want to use. Default: the first available certificate found in the Local Computer > Personal > Certificates area of the certificate store.

Examples

The following script installs and enables the SSL listener, using default values for all optional parameters.

```
Enable-VdaSSL –Enable
```

The following script installs and enables the SSL listener, and specifies SSL port 400, the GOV cipher suite, and a minimum TLS 1.2 SSL protocol value.

```
Enable-VdaSSL – Enable –SSLPort 400 ‘SSLMinVersion “TLS_1.2”
–SSLCipherSuite “GOV”
```

The following script disables the SSL listener on the VDA.

```
Enable-VdaSSL –Disable
```

Manually configure SSL on a VDA

When configuring SSL on a VDA manually, you grant generic read access to the SSL certificate’s private key for the appropriate service on each VDA: NT SERVICE\PorticaService for a VDA for Windows Desktop OS, or NT SERVICE\TermService for a VDA for Windows Server OS. On the machine where the VDA is installed:

1. Launch the Microsoft Management Console (MMC): Start > Run > mmc.exe.
2. Add the Certificates snap-in to the MMC:

1. Select File > Add/Remove Snap-in.
2. Select Certificates and then click Add.
3. When prompted with “This snap-in will always manage certificates for:” choose “Computer account” and then click Next.
4. When prompted with “Select the computer you want this snap-in to manage” choose “Local computer” and then click Finish.

3. Under Certificates (Local Computer) > Personal > Certificates, right–click the certificate and then select All Tasks > Manage Private Keys.
4. The Access Control List Editor displays “Permissions for (FriendlyName) private keys” where (FriendlyName) is the name of your SSL certificate. Add one of the following services and give it Read access:
   - For a VDA for Windows Desktop OS, "PORTICASERVICE"
   - For a VDA for Windows Server OS, "TERMSERVICE"
5. Double-click the installed SSL certificate. In the certificate dialog, select the Details tab and then scroll to the bottom. Click Thumbprint.
6. Run regedit and go to HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.
   1. Edit the SSL Thumbprint key and copy the value of the SSL certificate’s thumbprint into this binary value. You can safely ignore unknown items in the Edit Binary Value dialog box (such as '0000' and special characters).
   2. Edit the SSLEnabled key and change the DWORD value to 1. (To disable SSL later, change the DWORD value to 0.)
   3. If you want to change the default settings (optional), use the following in the same registry path:
      - SSLPort DWORD – SSL port number. Default: 443.
      - SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Default: 2 (TLS 1.0).
      - SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Default: 3 (ALL).
7. Ensure the SSL TCP port is open in the Windows Firewall if it is not the default 443. (When you create the inbound rule in Windows Firewall, make sure its properties have the "Allow the connection" and "Enabled" entries selected.)
8. Ensure that no other applications or services (such as IIS) are using the SSL TCP port.
9. For VDAs for Windows Server OS, restart the machine for the changes to take effect. (You do not need to restart machines containing VDAs for Windows Desktop OS.)

Configure SSL on Delivery Groups

Complete this procedure for each Delivery Group that contains VDAs you have configured for SSL connections.

1. From Studio, open the PowerShell console.
2. Run asnp Citrix.* to load the Citrix product cmdlets.
3. Run Get-BrokerAccessPolicyRule –DesktopGroupName ‘<delivery-group-name>’ | Set-BrokerAccessPolicyRule –HdxSslEnabled $true.
   where <delivery-group-name> is the name of the Delivery Group containing VDAs.
4. Run Set-BrokerSite –DnsResolutionEnabled $true.

Troubleshooting

If a connection error occurs, check the VDA's system event log.

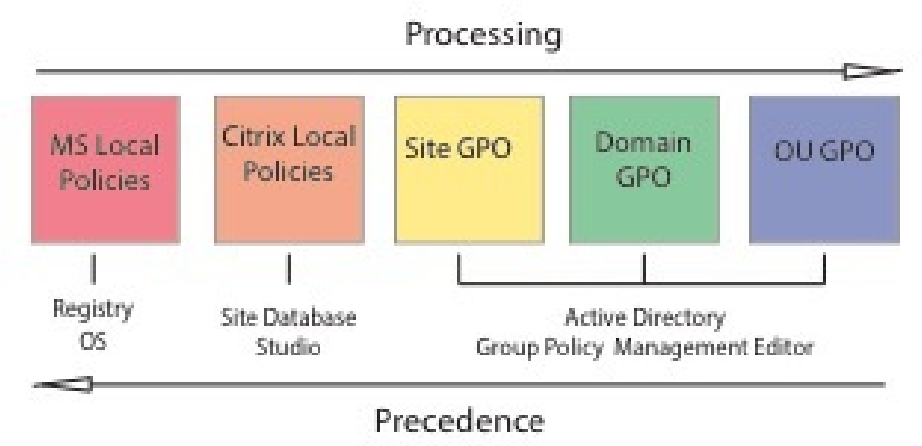
When using Receiver for Windows, if you receive a connection error (such as 1030) that indicates an SSL error, disable Desktop Viewer and then try connecting again; although the connection will still fail, an explanation of the underlying SSL issue might be provided (for example, you specified an incorrect template when requesting a certificate from the certificate authority).

Policies

Sep 29, 2015

Policies are a collection of settings that define how sessions, bandwidth, and security are managed for a group of users, devices, or connection types.

You can apply policy settings to physical and virtual machines or to users. You can apply settings to individual users at the local level or in security groups in Active Directory. The configurations define specific criteria and rules, and if you do not specifically assign the policies, the settings are applied to all connections.



You can apply policies on different levels of the network. Policy settings placed at the Organizational Unit GPO level take the highest precedence on the network. Policies at the Domain GPO level override policies on the Site Group Policy Object level, which override any conflicting policies on both the Microsoft and Citrix Local Policies levels.

All Citrix Local Policies are created and managed in the Citrix Studio console and stored in the Site Database; whereas, Group Policies are created and managed with the Microsoft Group Policy Management Console (GPMC) and stored in Active Directory. Microsoft Local Policies are created in the Windows Operating System and are stored in the registry.

Studio uses a Modeling Wizard to help administrators compare configuration settings within templates and policies to help eliminate conflicting and redundant settings. Administrators can set GPOs using the GPMC to configure settings and apply them to a target set of users at different levels of the network.

These GPOs are saved in Active Directory, and access to the management of these settings is generally restricted for most of IT for security.

Settings are merged according to priority and their condition. Any disabled setting overrides a lower-ranked enabled setting. Unconfigured policy settings are ignored and do not override lower-ranked settings.

Local policies can also have conflicts with group policies in the Active Directory, which could override each other depending on the situation.

All policies are processed in the following order:

1. The end user logs on to a machine using domain credentials.
2. Credentials are sent to the domain controller.
3. Active Directory applies all policies (end user, endpoint, organizational unit, and domain).
4. The end user logs on to Receiver and accesses an application or desktop.

5. Citrix and Microsoft policies are processed for the end user and machine hosting the resource.
6. Active Directory determines precedence for policy settings and applies them to the registries of the endpoint device and to the machine hosting the resource.
7. The end user logs off from the resource. Citrix policies for the end user and endpoint device are no longer active.
8. The end user logs off the user device, which releases the GPO user policies.
9. The end user turns off the device, which releases the GPO machine policies.

When creating policies for groups of users, devices, and machines, some members may have different requirements and would need exceptions to some policy settings. Exceptions are made by way of filters in Studio and the GPMC that determine who or what the policy affects.

Related content

- Work with policies
- Policy templates
- Create policies
- Compare, prioritize, model, and troubleshoot policies
- Default policy settings
- Policy settings reference

Work with policies

Sep 29, 2015

Configure Citrix policies to control user access and session environments. Citrix policies are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of users, devices, or connection types. Each policy can contain multiple settings.

Tools for working with Citrix policies

You can use the following tools to work with Citrix policies.

- **Studio** - If you are a Citrix administrator without permission to manage group policy, use Studio to create policies for your site. Policies created using Studio are stored in the site database and updates are pushed to the virtual desktop either when that virtual desktop registers with the broker or when a user connects to that virtual desktop.
- **Local Group Policy Editor** (Microsoft Management Console snap-in) - If your network environment uses Active Directory and you have permission to manage group policy, you can use the Local Group Policy Editor to create policies for your Site. The settings you configure affect the Group Policy Objects (GPOs) you specify in the Group Policy Management Console.
  Important: You must use the Local Group Policy Editor to configure some policy settings, including those related to registering VDAs with a Controller and those related to Microsoft App-V servers.

Policy processing order and precedence

Group policy settings are processed in the following order:

1. Local GPO
2. XenApp or XenDesktop Site GPO (stored in the Site database)
3. Site-level GPOs
4. Domain-level GPOs
5. Organizational Units

However, if a conflict occurs, policy settings that are processed last can overwrite those that are processed earlier. This means that policy settings take precedence in the following order:

1. Organizational Units
2. Domain-level GPOs
3. Site-level GPOs
4. XenApp or XenDesktop Site GPO (stored in the Site database)
5. Local GPO

For example, a Citrix administrator uses Studio to create a policy (Policy A) that enables client file redirection for the company's sales employees. Meanwhile, another administrator uses the Group Policy Editor to create a policy (Policy B) that disables client file redirection for sales employees. When the sales employees log on to the virtual desktops, Policy B is applied and Policy A is ignored because Policy B was processed at the domain level and Policy A was processed at the XenApp or XenDesktop Site GPO level.

However, when a user launches an ICA or Remote Desktop Protocol (RDP) session, Citrix session settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This includes settings that are related to typical RDP client connection settings such as Desktop wallpaper, Menu animation, and View window contents while dragging.

When using multiple policies, you can prioritize policies that contain conflicting settings; see Compare, prioritize, model, and troubleshoot policies for details.

Workflow for Citrix policies

The process for configuring policies is as follows:

1. Create the policy.
2. Configure policy settings.
3. Assign the policy to machine and user objects.
4. Prioritize the policy.
5. Verify the effective policy by running the Citrix Group Policy Modeling wizard.

Navigate Citrix policies and settings

In the Local Group Policy Editor, policies and settings appear in two categories: Computer Configuration and User Configuration. Each category has a Citrix Policies node. See the Microsoft documentation for details about navigating and using this snap-in.

In Studio, policy settings are sorted into categories based on the functionality or feature they affect. For example, the Profile management section contains policy settings for Profile management.

- Computer settings (policy settings applying to machines) define the behavior of virtual desktops and are applied when a virtual desktop starts. These settings apply even when there are no active user sessions on the virtual desktop. User settings define the user experience when connecting using ICA. User policies are applied when a user connects or reconnects using ICA. User policies are not applied if a user connects using RDP or logs on directly to the console.
  To access policies, settings, or templates, select Policies in the Studio navigation pane.
  - The **Policies** tab lists all policies. When you select a policy, tabs to the right display: Overview (name, priority, enabled/disabled status, and description), Settings (list of configured settings), and Assigned to (user and machine objects to which the policy is currently assigned). For more information, see Create policies.
  - The **Templates** tab lists Citrix-provided and custom templates you created. When you select a template, tabs to the right display: Description (why you might want to use the template) and Settings (list of configured settings). For more information, see Policy templates.
  - The **Comparison** tab enables you to compare the settings in a policy or template with those in other policies or templates. For example, you might want to verify setting values to ensure compliance with best practices. For more information, see Compare, prioritize, model, and troubleshoot policies.
  - From the **Modelling** tab, you can simulate connection scenarios with Citrix policies. For more information, see Compare, prioritize, model, and troubleshoot policies.

  To search for a setting in a policy or template:
  1. Select the policy or template.
  2. Select Edit policy or Edit Template in the Actions pane.
  3. On the Settings page, begin to type the name of the setting.

  You can refine your search by selecting a specific product version, selecting a category (for example, Bandwidth), or by selecting the View selected only check box or selecting to search only the settings that have been added to the selected policy. For an unfiltered search, select All Settings.

- To search for a setting within a policy :
  1. Select the policy.
  2. Select the Settings tab, begin to type the name of the setting.

You can refine your search by selecting a specific product version or by selecting a category. For an unfiltered search, select

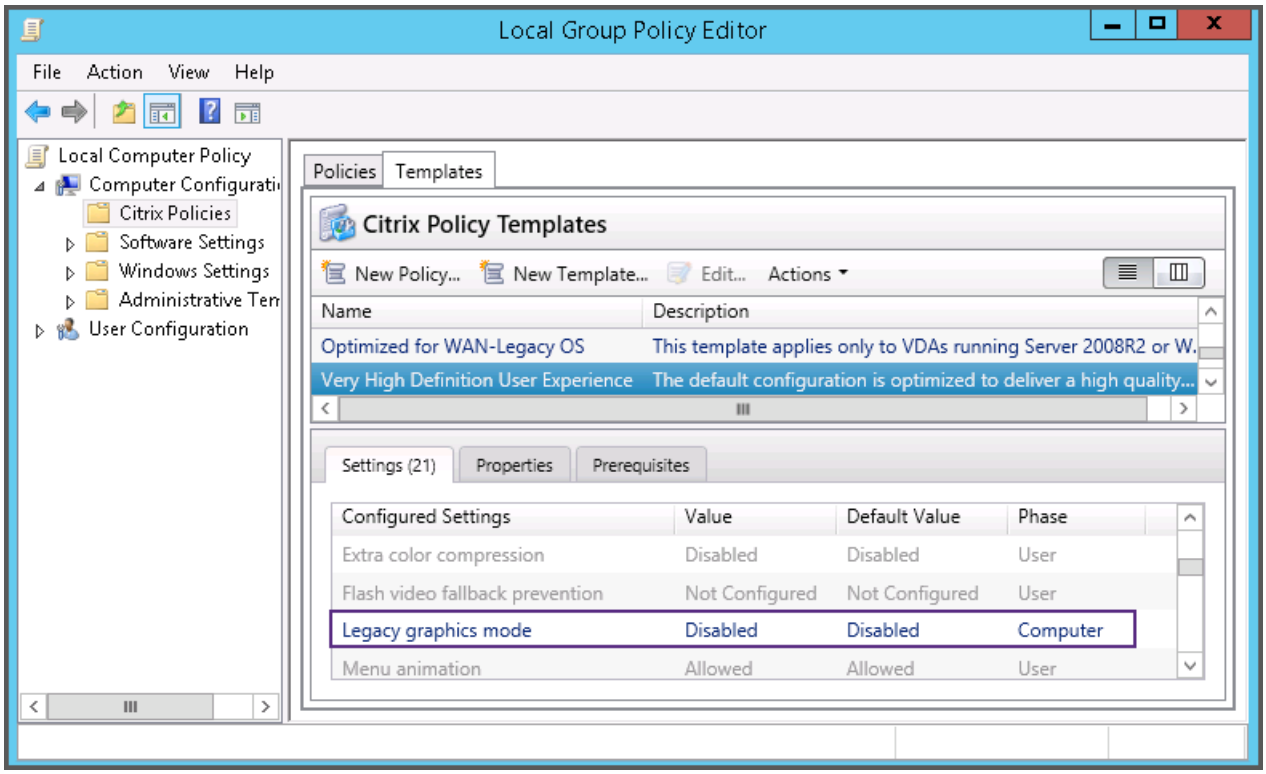
All Settings.

A policy, once created, is completely independent of the template used. You can use the Description field on a new policy to keep track of the source template used.

In Studio, policies and templates are displayed in a single list regardless of whether they contain user, computer or both types of settings and can be applied using both user and computer filters.

In Group Policy Editor, Computer and User settings must be applied separately, even if created from a template that contains both types of settings. In this example choosing to use Very High Definition User Experience in Computer Configuration:

- Legacy Graphics mode is a Computer setting that will be used in a policy created from this template.
- The User settings, grayed out, will not be used in a policy created from this template.



Policy templates

Nov 06, 2015

Templates are a source for creating policies from a predefined starting point. Built-in Citrix templates, optimized for specific environments or network conditions, can be used as:

- A source for creating your own policies and templates to share between sites.
- A reference for easier comparison of results between deployments as you will be able to quote the results, for example, "..when using Citrix template x or y..".
- A method for communicating policies with Citrix Support or trusted third parties by importing or exporting templates.

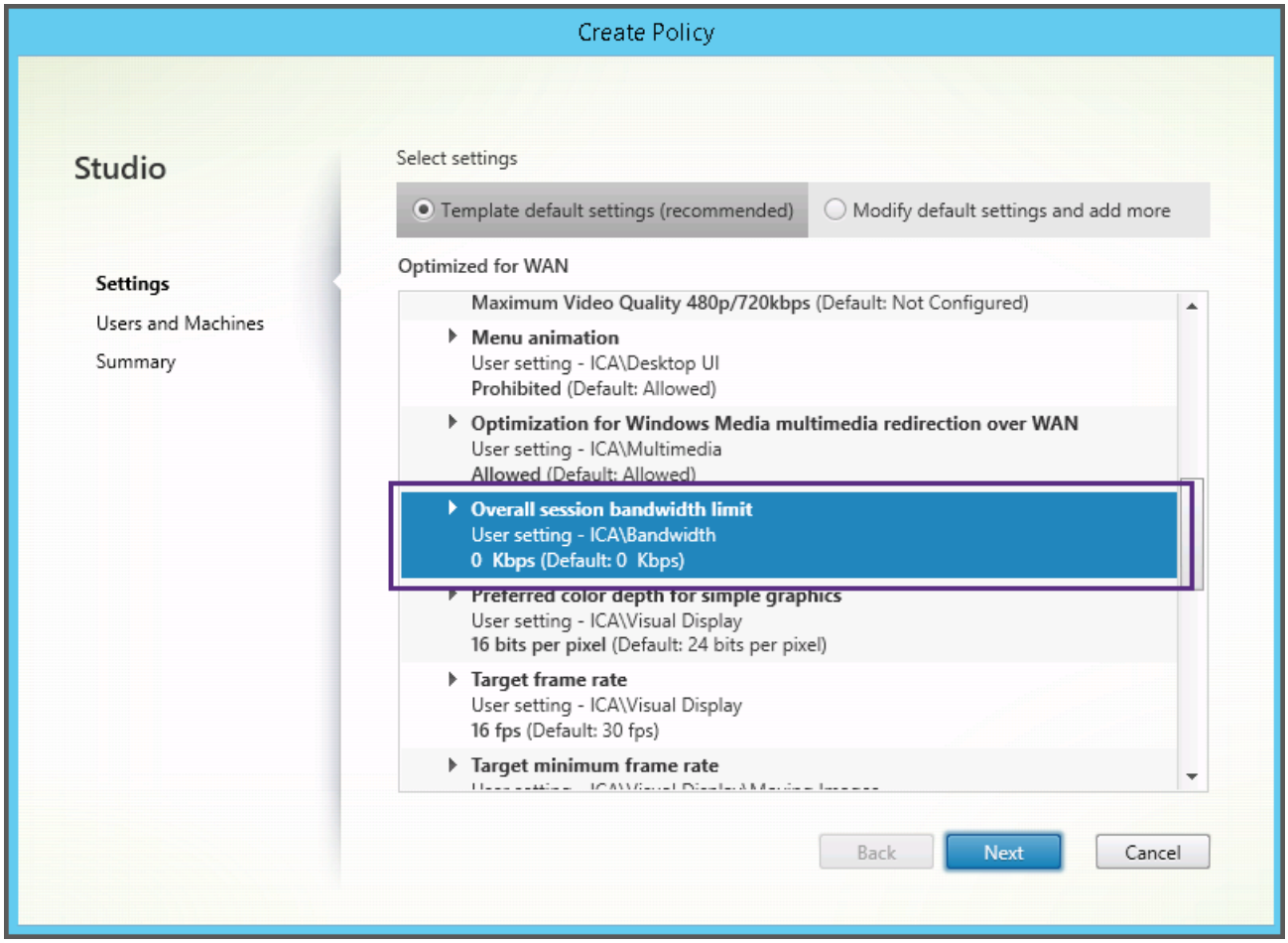
Policy templates can be imported or exported. For additional templates and updates to the built-in templates, see CTX202000.
For considerations when using templates to create policies, see CTX202330.

Built-in Citrix templates in 7.6 FP3

The XenApp and XenDesktop 7.6 FP3 Group Policy Management package (2.5.0.0) includes the following policy templates that replace and enhance the previously available built-in Citrix templates:

- **Very High Definition User Experience**. This template enforces default settings which maximize the user experience. Use this template in scenarios where multiple policies are processed in order of precedence.
- **High Server Scalability**. Apply this template to economize on server resources. This template balances user experience and server scalability. It offers a good user experience while increasing the number of users you can host on a single server. This template does not use video codec for compression of graphics and prevents server side multimedia rendering.
- **High Server Scalability-Legacy OS**. This High Server Scalability template applies only to VDAs running Server 2008 R2 or Windows 7 and earlier. This template relies on the Legacy graphics mode which is more efficient for those operating systems.
- **Optimized for WAN**. This template is intended for task workers in branch offices using a shared WAN connection or remote locations with low bandwidth connections accessing applications with graphically simple user interfaces with little multimedia content. This template trades off video playback experience and some server scalability for optimized bandwidth efficiency.
- **Optimized for WAN-Legacy OS**. This Optimized for WAN template applies only to VDAs running Server 2008 R2 or Windows 7 and earlier. This template relies on the Legacy graphics mode which is more efficient for those operating systems.
- **Security and Control**. Use this template in environments with low tolerance to risk, to minimize the features enabled by default in XenApp and XenDesktop. This template includes settings which will disable access to printing, clipboard, peripheral devices, drive mapping, port redirection, and Flash acceleration on user devices. Applying this template may use more bandwidth and reduce user density per server.

While we recommend using the built-in Citrix templates with their default settings, you will find settings that do not have a specific recommended value. For example, Overall session bandwidth limit, included in the Optimized for WAN templates. In this case, the template takes the approach of exposing the setting so the administrator will understand this setting is likely to apply to the scenario.



If you are working with a deployment (policy management and VDAs) prior to XenApp and XenDesktop 7.6 FP3, and require High Server Scalability and Optimized for WAN templates, please use the Legacy OS versions of these templates when these apply.

> ## Note
>
> Built-in templates are created and updated by Citrix. You cannot modify or delete these templates.

Create and manage templates using Studio

To create a new template based on a template:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Templates** tab and then select the template from which you will create the new template.
3. Select **Create Template** in the Actions pane.
4. Select and configure the policy settings to include in the template. Remove any existing settings that should not be included. Enter a name for the template.

After you click **Finish**, the new template appears on the **Templates** tab.

To create a new template based on a policy:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Policies** tab and then select the policy from which you will create the new template.
3. Select **Save as Template** in the Actions pane.
4. Select and configure any new policy settings to include in the template. Remove any existing settings that should not be included. Enter a name and description for the template, and then click **Finish**.

To import a template:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Templates** tab and then select **Import Template**.
3. Select the template file to import and then click **Open**. If you import a template with the same name as an existing template, you can choose to overwrite the existing template or save the template with a different name that is generated automatically.

To export a template:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Templates** tab and then select **Export Template**.
3. Select the location where you want to save the template and then click **Save**.

A .gpt file is created in the specified location.

Create and manage templates using the Group Policy Editor

From the Group Policy Editor, expand Computer Configuration or User Configuration. Expand the Policies node and then select Citrix Policies. Choose the appropriate action below.

Task	Instruction
Create a new template from an existing policy	On the Policies tab, select the policy and then select Actions > Save as Template.
Create a new policy from an existing template	On the Templates tab, select the template and then click New Policy.
Create a new template from an existing template	On the Templates tab, select the template and then click New Template.
Import a template	On the Templates tab, select Actions > Import.
Export a template	On the Templates tab, select Actions > Export.
View template settings	On the Templates tab, select the template and then click the Settings tab.
View a summary of template properties	On the Templates tab, select the template and then click the Properties tab.
View template prerequisites	On the Templates tab, select the template and then click the Prerequisites tab.

Templates and Delegated Administration

Policy templates are stored on the machine where the policy management package was installed. This machine is either the Delivery Controller machine or the Group Policy Objects management machine - not the XenApp and XenDesktop Site's database. This means that the policy template files are controlled by Windows administrative permissions rather than Site's Delegated Administration roles and scopes.

As a result, an administrator with read-only permission in the Site can, for example, create new templates. However, because templates are local files, no changes are actually made to your environment.

Custom templates are only visible to the user account that creates them and stored in the user's Windows profile. To expose a custom template further, create a policy from it or export it to a shared location.

Create policies

Sep 22, 2015

Before creating a policy, decide which group of users or devices it should affect. You may want to create a policy based on user job function, connection type, user device, or geographic location. Alternatively, you can use the same criteria that you use for Windows Active Directory group policies.

If you already created a policy that applies to a group, consider editing that policy and configuring the appropriate settings, instead of creating another policy. Avoid creating a new policy solely to enable a specific setting or to exclude the policy from applying to certain users.

When you create a new policy, you can base it on settings in a policy template and customize settings as needed, or you can create it without using a template and add all the settings you need.

Policy settings

Policy settings can be enabled, disabled, or not configured. By default, policy settings are not configured, which means they are not added to a policy. Settings are applied only when they are added to a policy.

Some policy settings can be in one of the following states:

- Allowed or Prohibited allows or prevents the action controlled by the setting. In some cases, users are allowed or prevented from managing the setting's action in a session. For example, if the Menu animation setting is set to Allowed, users can control menu animations in their client environment.
- Enabled or Disabled turns the setting on or off. If you disable a setting, it is not enabled in lower-ranked policies.

In addition, some settings control the effectiveness of dependent settings. For example, Client drive redirection controls whether or not users are allowed to access the drives on their devices. To allow users to access their network drives, both this setting and the Client network drives setting must be added to the policy. If the Client drive redirection setting is disabled, users cannot access their network drives, even if the Client network drives setting is enabled.

In general, policy setting changes that impact machines go into effect either when the virtual desktop restarts or when a user logs on. Policy setting changes that impact users go into effect the next time users log on. If you are using Active Directory, policy settings are updated when Active Directory re-evaluates policies at 90-minute intervals and applied either when the virtual desktop restarts or when a user logs on.

For some policy settings, you can enter or select a value when you add the setting to a policy. You can limit configuration of the setting by selecting Use default value; this disables configuration of the setting and allows only the setting's default value to be used when the policy is applied, regardless of the value that was entered before selecting Use default value.

As best practice:

- Assign policies to groups rather than individual users. If you assign policies to groups, assignments are updated automatically when you add or remove users from the group.
- Do not enable conflicting or overlapping settings in Remote Desktop Session Host Configuration. In some cases, Remote Desktop Session Host Configuration provides similar functionality to Citrix policy settings. When possible, keep all settings consistent (enabled or disabled) for ease of troubleshooting.
- Disable unused policies. Policies with no settings added create unnecessary processing.

Policy assignments

When creating a policy, you assign it to certain user and machine objects; that policy is applied to connections according to specific criteria or rules. In general, you can add as many assignments as you want to a policy, based on a combination of criteria. If you specify no assignments, the policy is applied to all connections.

The following table lists the available assignments:

Assignment Name	Applies a policy based on
Access Control	Access control conditions through which a client is connecting. • Connection type - Whether to apply the policy to connections made with or without NetScaler Gateway. • NetScaler Gateway farm name - Name of the NetScaler Gateway virtual server. • Access condition - Name of the end point analysis policy or session policy to use.
Citrix CloudBridge	Whether or not a user session is launched through Citrix CloudBridge. Note: You can add only one Citrix CloudBridge assignment to a policy.
Client IP Address	IP address of the user device used to connect to the session. • IPv4 examples: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24 • IPv6 examples: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Client Name	Name of the user device. • Exact match: ClientABCName • Using wildcard: Client*Name
Delivery Group	Delivery Group membership.
Delivery Group type	Type of desktop or application: private desktop, shared desktop, private application, or shared application.
Organizational Unit (OU)	Organizational unit.
Tag	Tags. **Note:** To ensure that policies are applied correctly when using tags, install the hotfix at CTX142439.
User or Group	User or group name.

When a user logs on, all policies that match the assignments for the connection are identified. Those policies are sorted into priority order and multiple instances of any setting are compared. Each setting is applied according to the priority ranking of the policy. Any policy setting that is disabled takes precedence over a lower-ranked setting that is enabled. Policy

settings that are not configured are ignored.

Important: When configuring both Active Directory and Citrix policies using the Group Policy Management Console, assignments and settings may not be applied as expected. For more information, see CTX127461
A policy named "Unfiltered" is provided by default.

- If you use Studio to manage Citrix policies, settings you add to the Unfiltered policy are applied to all servers, desktops, and connections in a Site.
- If you use the Local Group Policy Editor to manage Citrix policies, settings you add to the Unfiltered policy are applied to all Sites and connections that are within the scope of the Group Policy Objects (GPOs) that contain the policy. For example, the Sales OU contains a GPO called Sales-US that includes all members of the US sales team. The Sales-US GPO is configured with an Unfiltered policy that includes several user policy settings. When the US Sales manager logs on to the Site, the settings in the Unfiltered policy are automatically applied to the session because the user is a member of the Sales-US GPO.

An assignment's mode determines if the policy is applied only to connections that match all the assignment criteria. If the mode is set to Allow (the default), the policy is applied only to connections that match the assignment criteria. If the mode is set to Deny, the policy is applied if the connection does not match the assignment criteria. The following examples illustrate how assignment modes affect Citrix policies when multiple assignments are present.

- **Example: Assignments of like type with differing modes** - In policies with two assignments of the same type, one set to Allow and one set to Deny, the assignment set to Deny takes precedence, provided the connection satisfies both assignments. For example:
  Policy 1 includes the following assignments:
  - Assignment A specifies the Sales group; the mode is set to Allow
  - Assignment B specifies the Sales manager's account; the mode is set to Deny

  Because the mode for Assignment B is set to Deny, the policy is not applied when the Sales manager logs on to the Site, even though the user is a member of the Sales group.

- **Example: Assignments of differing type with like modes** - In policies with two or more assignments of differing types, set to Allow, the connection must satisfy at least one assignment of each type in order for the policy to be applied. For example:
  Policy 2 includes the following assignments:
  - Assignment C is a User assignment that specifies the Sales group; the mode is set to Allow
  - Assignment D is a Client IP Address assignment that specifies 10.8.169.* (the corporate network); the mode is set to Allow

  When the Sales manager logs on to the Site from the office, the policy is applied because the connection satisfies both assignments.

  Policy 3 includes the following assignments:
  - Assignment E is a User assignment that specifies the Sales group; the mode is set to Allow
  - Assignment F is an Access Control assignment that specifies NetScaler Gateway connection conditions; the mode is set to Allow

  When the Sales manager logs on to the Site from the office, the policy is not applied because the connection does not satisfy Assignment F.

Create a new policy based on a template, using Studio

1. Select Policies in the Studio navigation pane.
2. Select the Templates tab and select a template.
3. Select Create Policy from Template in the Actions pane.

4. By default, the new policy uses all the default settings in the template (the Use template default settings radio button is selected). If you want to change settings, select the Modify defaults and add more settings radio button, and then add or remove settings.
5. Specify how to apply the policy by selecting one of the following:
   - Assign to selected user and machine objects and then select the user and machine objects to which the policy will apply.
   - Assign to all objects in a site to apply the policy to all user and machine objects in the Site.
6. Enter a name for the policy (or accept the default); consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.
   The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you need to prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

Create a new policy using Studio

1. Select Policies in the Studio navigation pane.
2. Select the Policies tab.
3. Select Create Policy in the Actions pane.
4. Add and configure policy settings.
5. Specify how to apply the policy by choosing one of the following:
   - Assign to selected user and machine objects and then select the user and machine objects to which the policy will apply.
   - Assign to all objects in a site to apply the policy to all user and machine objects in the Site.
6. Enter a name for the policy (or accept the default); consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.
   The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you need to prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

Create and manage policies using the Group Policy Editor

From the Group Policy Editor, expand Computer Configuration or User Configuration. Expand the Policies node and then select Citrix Policies. Choose the appropriate action below.

Task	Instruction
Create a new policy	On the Policies tab, click New.
Edit an existing policy	On the Policies tab, select the policy and then click Edit.
Change the priority of an existing policy	On the Policies tab, select the policy and then click either Higher or Lower.
View summary information about a policy	On the Policies tab, select the policy and then click the Summary tab.
View and amend policy settings	On the Policies tab, select the policy and then click the Settings tab.

Task	Instruction
View and amend policy filters	On the Policies tab, select the policy and then click the Filters tab.
Enable or disable a policy	On the Policies tab, select the policy and then select either Actions > Enable or Actions > Disable.
Create a new policy from an existing template	On the Templates tab, select the template and then click New Policy.

Compare, prioritize, model, and troubleshoot policies

Sep 16, 2016

You can use multiple policies to customize your environment to meet users' needs based on their job functions, geographic locations, or connection types. For example, for security you may need to place restrictions on user groups who regularly work with sensitive data. You can create a policy that prevents users from saving sensitive files on their local client drives. However, if some people in the user group do need access to their local drives, you can create another policy for only those users. You then rank or prioritize the two policies to control which one takes precedence.

When using multiple policies, you must determine how to prioritize them, how to create exceptions, and how to view the effective policy when policies conflict.

In general, policies override similar settings configured for the entire Site, for specific Delivery Controllers, or on the user device. The exception to this principle is security. The highest encryption setting in your environment, including the operating system and the most restrictive shadowing setting, always overrides other settings and policies.

Citrix policies interact with policies you set in your operating system. In a Citrix environment, Citrix settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This includes settings that are related to typical Remote Desktop Protocol (RDP) client connection settings such as Desktop wallpaper, Menu animation, and View window contents while dragging. For some policy settings, such as Secure ICA, the settings in policies must match the settings in the operating system. If a higher priority encryption level is set elsewhere, the Secure ICA policy settings that you specify in the policy or when you are delivering application and desktops can be overridden.

For example, the encryption settings that you specify when creating Delivery Groups should be at the same level as the encryption settings you specified throughout your environment.

Note: In the second hop of double-hop scenarios, when a Desktop OS VDA connects to Server OS VDA, Citrix policies act on the Desktop OS VDA as if it were the user device. For example, if policies are set to cache images on the user device, the images cached for the second hop in a double-hop scenario are cached on the Desktop OS VDA machine.

Compare policies and templates

You can compare settings in a policy or template with those in other policies or templates. For example, you might need to verify setting values to ensure compliance with best practices. You might also want to compare settings in a policy or template with the default settings provided by Citrix.

1. Select Policies in the Studio navigation pane.
2. Click the Comparison tab and then click Select.
3. Choose the policies or templates to compare. To include default values in the comparison, select the Compare to default settings check box.
4. After you click Compare, the configured settings are displayed in columns.
5. To see all settings, select Show All Settings. To return to the default view, select Show Common Settings.

Prioritize policies

Prioritizing policies allows you to define the precedence of policies when they contain conflicting settings. When a user logs on, all policies that match the assignments for the connection are identified. Those policies are sorted into priority order and multiple instances of any setting are compared. Each setting is applied according to the priority ranking of the policy.

You prioritize policies by giving them different priority numbers in Studio. By default, new policies are given the lowest priority. If policy settings conflict, a policy with a higher priority (a priority number of 1 is the highest) overrides a policy with a

lower priority. Settings are merged according to priority and the setting's condition; for example, whether the setting is disabled or enabled. Any disabled setting overrides a lower-ranked setting that is enabled. Policy settings that are not configured are ignored and do not override the settings of lower-ranked settings.

1. Select Policies in the Studio navigation pane. Make sure the Policies tab is selected.
2. Select a policy.
3. Select Lower Priority or Higher Priority in the Actions pane.

Exceptions

When you create policies for groups of users, user devices, or machines, you may find that some members of the group require exceptions to some policy settings. You can create exceptions by:

- Creating a policy only for those group members who need the exceptions and then ranking the policy higher than the policy for the entire group
- Using the Deny mode for an assignment added to the policy

An assignment with the mode set to Deny applies a policy only to connections that do not match the assignment criteria. For example, a policy contains the following assignments:

- Assignment A is a client IP address assignment that specifies the range 208.77.88.*; the mode is set to Allow
- Assignment B is a user assignment that specifies a particular user account; the mode is set to Deny

The policy is applied to all users who log on to the Site with IP addresses in the range specified in Assignment A. However, the policy is not applied to the user logging on to the Site with the user account specified in Assignment B, even though the user's computer is assigned an IP address in the range specified in Assignment A.

Determine which policies apply to a connection

Sometimes a connection does not respond as expected because multiple policies apply. If a higher priority policy applies to a connection, it can override the settings you configure in the original policy. You can determine how final policy settings are merged for a connection by calculating the Resultant Set of Policy.

You can calculate the Resultant Set of Policy in the following ways:

- Use the Citrix Group Policy Modeling Wizard to simulate a connection scenario and discern how Citrix policies might be applied. You can specify conditions for a connection scenario such as domain controller, users, Citrix policy assignment evidence values, and simulated environment settings such as slow network connection. The report that the wizard produces lists the Citrix policies that would likely take effect in the scenario. If you are logged on to the Controller as a domain user, the wizard calculates the Resultant Set of Policy using both site policy settings and Active Directory Group Policy Objects (GPOs).
- Use Group Policy Results to produce a report describing the Citrix policies in effect for a given user and controller. The Group Policy Results tool helps you evaluate the current state of GPOs in your environment and generates a report that describes how these objects, including Citrix policies, are currently being applied to a particular user and controller.

You can launch the Citrix Group Policy Modeling Wizard from the Actions pane in Studio. You can launch either tool from the Group Policy Management Console in Windows.

If you run the Citrix Group Policy Modeling Wizard or Group Policy Results tool from the Group Policy Management Console, site policy settings created using Studio are not included in the Resultant Set of Policy.

To ensure you obtain the most comprehensive Resultant Set of Policy, Citrix recommends launching the Citrix Group Policy Modeling wizard from Studio, unless you create policies using only the Group Policy Management Console.

Use the Citrix Group Policy Modeling Wizard

Open the Citrix Group Policy Modeling Wizard using one of the following:

- Select Policies in the Studio navigation pane, select the Modeling tab, and then select Launch Modeling Wizard in the Actions pane.
- Launch the Group Policy Management Console (gpmc.msc), right-click Citrix Group Policy Modeling in the tree pane, and then select Citrix Group Policy Modeling Wizard.

Follow the wizard instructions to select the domain controller, users, computers, environment settings, and Citrix assignment criteria to use in the simulation. After you click Finish, the wizard produces a report of the modeling results. In Studio, the report appears in the middle pane under the Modeling tab.

To view the report, select View Modeling Report.

Troubleshoot policies

Users, IP addresses, and other assigned objects can have multiple policies that apply simultaneously. This can result in conflicts where a policy may not behave as expected. When you run the Citrix Group Policy Modeling Wizard or the Group Policy Results tool, you might discover that no policies are applied to user connections. When this happens, users connecting to their applications and desktops under conditions that match the policy evaluation criteria are not affected by any policy settings. This occurs when:

- No policies have assignments that match the policy evaluation criteria.
- Policies that match the assignment do not have any settings configured.
- Policies that match the assignment are disabled.

If you want to apply policy settings to the connections that meet the specified criteria, make sure:

- The policies you want to apply to those connections are enabled.
- The policies you want to apply have the appropriate settings configured.

Default policy settings

Aug 08, 2016

The following tables list policy settings, their default, and the Virtual Delivery Agent (VDA) versions to which they apply.

ICA

Name	Default setting	VDA
Client clipboard redirection	Allowed	All VDA versions
Desktop launches	Prohibited	VDA for Server OS 7 through current VDA for Server OS
ICA listener connection timeout	120000 milliseconds	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current VDA for Desktop OS
ICA listener port number	1494	All VDA versions
Launching of non-published programs during client connection	Prohibited	VDA for Server OS 7 through current VDA for Server OS
Client clipboard write allowed formats	No formats are specified	VDA 7.6
Restrict client clipboard write	Prohibited	VDA 7.6
Restrict session clipboard write	Prohibited	VDA 7.6
Session clipboard write allowed formats	No formats are specified	VDA 7.6

ICA/Adobe Flash Delivery/Flash Redirection

Name	Default setting	VDA
Flash video fallback prevention	Not configured	VDA 7.6 FP3
Flash video fallback prevention error *.swf		VDA 7.6 FP3

ICA/Audio

Name	Default setting	VDA

Name	Default setting	VDA
Audio Plug N Play	Allowed	VDA for Server OS 7 through current VDA for Server OS
Audio quality	High - high definition audio	All VDA versions
Client audio redirection	Allowed	All VDA versions
Client microphone redirection	Allowed	All VDA versions

ICA/Auto Client Reconnect

Name	Default setting	VDA
Auto client reconnect	Allowed	VDA
Auto client reconnect authentication	Do not require authentication	VDA
Auto client reconnect logging	Do not log auto-reconnect events	VDA

ICA/Bandwidth

Name	Default setting	VDA
Audio redirection bandwidth limit	0 Kbps	VDA
Audio redirection bandwidth limit percent	0	VDA
Client USB device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Client USB device redirection bandwidth limit percent	0	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Clipboard redirection bandwidth limit	0 Kbps	All VDA versions
Clipboard redirection bandwidth limit percent	0	All VDA versions
COM port redirection bandwidth limit	0 Kbps	All VDA versions; for VDA 7.x, configure this setting using the registry.
COM port redirection bandwidth limit percent	0	All VDA versions; for VDA 7.x, configure this setting using the registry.

Name	Default setting	VDA
File redirection bandwidth limit	0 Kbps	All VDA versions
File redirection bandwidth limit percent	0	All VDA versions
HDX MediaStream Multimedia Acceleration bandwidth limit	0 Kbps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
HDX MediaStream Multimedia Acceleration bandwidth limit percent	0	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
LPT port redirection bandwidth limit	0 Kbps	All VDA versions; for VDA 7.x, configure this setting using the registry.
LPT port redirection bandwidth limit percent	0	All VDA versions; for VDA 7.x, configure this setting using the registry.
Overall session bandwidth limit	0 Kbps	All VDA versions
Printer redirection bandwidth limit	0 Kbps	All VDA versions
Printer redirection bandwidth limit percent	0	All VDA versions
TWAIN device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
TWAIN device redirection bandwidth limit percent	0	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS

ICA/Client Sensors

Name	Default setting	VDA
Allow applications to use the physical location of the client device	Prohibited	VDA 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS

ICA/Desktop UI

Name	Default setting	VDA
Desktop Composition Redirection	Disabled (7.6 FP3 through current) Enabled (5.6 through 7.6	VDA 5.6, VDA for Desktop OS 7 through current, VDA

Name	Default setting	VDA
	FP2)	
Desktop Composition Redirection graphics quality	Medium	VDA 5.6, VDA for Desktop OS 7 through current, VDA
Desktop wallpaper	Allowed	All VDA versions
Menu animation	Allowed	All VDA versions
View window contents while dragging	Allowed	All VDA versions

ICA/End User Monitoring

Name	Default setting	VDA
ICA round trip calculation	Enabled	All VDA versions
ICA round trip calculation interval	15 seconds	All VDA versions
ICA round trip calculations for idle connections	Disabled	All VDA versions

ICA/Enhanced Desktop Experience

Name	Default setting	VDA
Enhanced Desktop Experience	Allowed	VDA for Server OS 7 through current VDA for Server OS

ICA/File Redirection

Name	Default setting	VDA
Auto connect client drives	Allowed	All VDA versions
Client drive redirection	Allowed	All VDA versions
Client fixed drives	Allowed	All VDA versions
Client floppy drives	Allowed	All VDA versions

Name	Default setting	VDA
Client network drives	Allowed	All VDA versions
Client optical drives	Allowed	All VDA versions
Client removable drives	Allowed	All VDA versions
Host to client redirection	Disabled	VDA for Server OS 7 through current VDA for Server OS
Preserve client drive letters	Disabled	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current VDA for Desktop OS
Read-only client drive access	Disabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Special folder redirection	Allowed	Web Interface deployments only; VDA for Server OS 7 through current VDA for Server OS
Use asynchronous writes	Disabled	All VDA versions

ICA/Graphics

Name	Default setting	VDA
Display memory limit	65536 Kb	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current VDA for Desktop OS
Display mode degrade preference	Degrade color depth first	All VDA versions
Dynamic windows preview	Enabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Image caching	Enabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Legacy graphics mode	Disabled	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Maximum allowed color depth	32 bits per pixel	All VDA versions
Notify user when	Disabled	VDA for Server OS 7 through current VDA for Server OS

Name	Default setting	VDA
display mode is degraded		
Queuing and tossing	Enabled	All VDA versions

ICA/Graphics/Caching

Name	Default setting	VDA
Persistent cache threshold	3000000 bps	VDA for Server OS 7 through current VDA for Server OS

ICA/Keep Alive

Name	Default setting	VDA
ICA keep alive timeout	60 seconds	All VDA versions
ICA keep alives	Do not send ICA keep alive messages	All VDA versions

ICA/Local App Access

Name	Default setting	VDA
Allow local app access	Prohibited	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
URL redirection black list	No sites are specified	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
URL redirection white list	No sites are specified	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS

ICA/Mobile Experience

Name	Default setting	VDA
Automatic keyboard display	Prohibited	VDA 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Launch touch-optimized desktop	Allowed	VDA 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS This setting is disabled and not available for Windows 10 machines.

Name	Default setting	VDA
Remote the combo box	Prohibited	VDA 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS

ICA/Multimedia

Name	Default setting	VDA
Limit video quality	Not configured	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Multimedia conferencing	Allowed	All VDA versions
Optimization for Windows Media multimedia redirection over WAN	Allowed	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Use GPU for optimizing Windows Media multimedia redirection over WAN	Prohibited	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Video load management policy setting	Not configured	VDA 7.6 FP3
Windows Media client-side content fetching	Allowed	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Windows Media Redirection	Allowed	All VDA versions
Windows Media Redirection buffer size	5 seconds	VDA 5, 5.5, and 5.6, Feature Pack 1
Windows Media Redirection buffer size use	Disabled	VDA 5, 5.5, and 5.6, Feature Pack 1

ICA/Multi-Stream Connections

Name	Default setting	VDA
Audio over UDP	Allowed	VDA for Server OS 7 through current VDA for Server OS
Audio UDP port range	16500, 16509	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Multi-Port policy	Primary port (2598) has High Priority	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Multi-Stream computer setting	Disabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Multi-Stream user setting	Disabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS

ICA/Port Redirection

Name	Default setting	VDA
Auto connect client COM ports	Disabled	All VDA versions; for VDA 7.x, configure this setting using the registry.
Auto connect client LPT ports	Disabled	All VDA versions; for VDA 7.x, configure this setting using the registry.
Client COM port redirection	Prohibited	All VDA versions; for VDA 7.x, configure this setting using the registry.
Client LPT port redirection	Prohibited	All VDA versions; for VDA 7.x, configure this setting using the registry.

ICA/Printing

Name	Default setting	VDA
Client printer redirection	Allowed	All VDA versions
Default printer	Set default printer to the client's main printer	All VDA versions
Printer assignments	User's current printer is used as the default printer for the session	All VDA versions

Name	Default setting	VDA
Printer auto-creation event log preference	Log errors and warnings	All VDA versions
Session printers	No printers are specified	All VDA versions
Wait for printers to be created (desktop)	Disabled	All VDA versions

ICA/Printing/Client Printers

Name	Default setting	VDA
Auto-create client printers	Auto-create all client printers	All VDA versions
Auto-create generic universal printer	Disabled	All VDA versions
Client printer names	Standard printer names	All VDA versions
Direct connections to print servers	Enabled	All VDA versions
Printer driver mapping and compatibility	No rules are specified	All VDA versions
Printer properties retention	Held in profile only if not saved on client	All VDA versions
Retained and restored client printers	Allowed	VDA 5, 5,5 and 5.6 Feature Pack 1

ICA/Printing/Drivers

Name	Default setting	VDA
Automatic installation of in-box printer drivers	Enabled	All VDA versions
Universal driver preference	EMF; XPS; PCL5c; PCL4; PS	All VDA versions
Universal print driver usage	Use universal printing only if requested driver is unavailable	All VDA versions

ICA/Printing/Universal Print Server

Name	Default setting	VDA
Universal Print Server enable	Disabled	All VDA versions

Name	Default setting	VDA
Universal Print Server print data stream (CGP) port	7229	All VDA versions
Universal Print Server print stream input bandwidth limit (kpbs)	0	All VDA versions
Universal Print Server web service (HTTP/SOAP) port	8080	All VDA versions

ICA/Printing/Universal Printing

Name	Default setting	VDA
Universal printing EMF processing mode	Spool directly to printer	All VDA versions
Universal printing image compression limit	Best quality (lossless compression)	All VDA versions
Universal printing optimization defaults	Image Compression • Desired image quality = Standard quality • Enable heavyweight compression = False Image and Font Caching • Allow caching of embedded images = True • Allow caching of embedded fonts = True Allow non-administrators to modify these settings = False	All VDA versions
Universal printing preview preference	Do not use print preview for auto-created or generic universal printers	All VDA versions
Universal printing print quality limit	No limit	All VDA versions

ICA/Security

Name	Default setting	VDA
SecureICA minimum encryption level	Basic	VDA for Server OS 7 through current VDA for Server OS

ICA/Server Limits

Name	Default setting	VDA
Server idle timer interval	0 milliseconds	VDA for Server OS 7 through current VDA for Server OS

ICA/Session Limits

Name	Default setting	VDA
Disconnected session timer	Disabled	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current VDA for Desktop OS
Disconnected session timer interval	1440 minutes	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current VDA for Desktop OS
Session connection timer	Disabled	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current VDA for Desktop OS
Session connection timer interval	1440 minutes	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current VDA for Desktop OS
Session idle timer	Enabledf	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current VDA for Desktop OS
Session idle timer interval	1440 minutes	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current VDA for Desktop OS

ICA/Session Reliability

Name	Default setting	VDA
Session reliability connections	Allowed	All VDA versions
Session reliability port number	2598	All VDA versions
Session reliability timeout	180 seconds	All VDA versions

ICA/Time Zone Control

Name	Default setting	VDA
Estimate local time for legacy clients	Enabled	VDA for Server OS 7 through current VDA for Server OS
Use local time of client	Use server time zone	All VDA versions

ICA/TWAIN Devices

Name	Default setting	VDA
Client TWAIN device redirection	Allowed	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
TWAIN compression level	Medium	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS

ICA/USB Devices

Name	Default setting	VDA
Client USB device optimization rules	No rules are specified	VDA 7.6 FP3
Client USB device redirection	Prohibited	All VDA versions
Client USB device redirection rules	No rules are specified	All VDA versions
Client USB Plug and Play device redirection	Allowed	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS

ICA/Visual Display

Name	Default setting	VDA
Preferred color depth for simple graphics	24 bits per pixel	VDA 7.6 FP3
Target frame rate	30 fps	All VDA versions
Visual quality	Medium	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Use video codec for compression	Use video codec when available	VDA 7.6 FP3

ICA/Visual Display/Moving Images

Name	Default setting	VDA
Minimum image quality	Normal	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Moving image compression	Enabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Progressive compression level	None	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Progressive compression threshold value	2147483647 Kbps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Target minimum frame rate	10 fps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS

ICA/Visual Display/Still Images

Name	Default setting	VDA
Extra color compression	Disabled	All VDA versions
Extra color compression threshold	8192 Kbps	All VDA versions
Heavyweight compression	Disabled	All VDA versions
Lossy compression level	Medium	All VDA versions
Lossy compression threshold value	2147483647 Kbps	All VDA versions

ICA/WebSockets

Name	Default setting	VDA
WebSockets connections	Prohibited	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
WebSockets port number	8008	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
WebSockets trusted origin server list	The wildcard, *, is used to trust all Receiver for Web URLs	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS

Load Management

Name	Default setting	VDA
Concurrent logon tolerance	2	VDA for Server OS 7 through current VDA for Server OS
CPU usage	Disabled	VDA for Server OS 7 through current VDA for Server OS
CPU usage excluded process priority	Below Normal or Low	VDA for Server OS 7 through current VDA for Server OS
Disk usage	Disabled	VDA for Server OS 7 through current VDA for Server OS
Maximum number of sessions	250	VDA for Server OS 7 through current VDA for Server OS
Memory usage	Disabled	VDA for Server OS 7 through current VDA for Server OS
Memory usage base load	Zero load: 768MB	VDA for Server OS 7 through current VDA for Server OS

Profile Managment/Advanced settings

Name	Default setting	VDA
Disable automatic configuration	Disabled	All VDA versions
Log off user if a problem is encountered	Disabled	All VDA versions
Number of retries when accessing locked files	5	All VDA versions
Process Internet cookie files on logoff	Disabled	All VDA versions

Profile Management/Basic settings

Name	Default setting	VDA
Active write back	Disabled	All VDA versions
Enable Profile management	Disabled	All VDA versions
Excluded groups	Disabled. Members of all user groups are processed.	All VDA versions
Offline profile support	Disabled	All VDA versions

Name	Default setting	VDA
Path to user store	Windows	All VDA versions
Process logons of local administrators	Disabled	All VDA versions
Processed groups	Disabled. Members of all user groups are processed.	All VDA versions

Profile Management/Cross-Platform Settings

Name	Default setting	VDA
Cross-platform settings user groups	Disabled. All user groups specified in Processed groups are processed	All VDA versions
Enable cross-platform settings	Disabled	All VDA versions
Path to cross-platform definitions	Disabled. No path is specified.	All VDA versions
Path to cross-platform settings store	Disabled. Windows\PM_CM is used.	All VDA versions
Source for creating cross-platform settings	Disabled	All VDA versions

Profile Management/File System/Exclusions

Name	Default setting	VDA
Exclusion list - directories	Disabled. All folders in the user profile are synchronized.	All VDA versions
Exclusion list - files	Disabled. All files in the user profile are synchronized.	All VDA versions

Profile Management/File System/Synchronization

Name	Default setting	VDA
Directories to synchronize	Disabled. Only non-excluded folders are synchronized.	All VDA versions
Files to synchronize	Disabled. Only non-excluded files are synchronized.	All VDA versions
Folders to mirror	Disabled. No folders are mirrored.	All VDA versions

Profile Management/Folder Redirection

Name	Default setting	VDA
Grant administrator access	Disabled	All VDA versions
Include domain name	Disabled	All VDA versions

Profile Management/Folder Redirection/AppData(Roaming)

Name	Default setting	VDA
AppData(Roaming) path	Disabled. No location is specified.	All VDA versions
Redirection settings for AppData(Roaming)	Contents are redirected to the UNC path specified in the AppData(Roaming) path policy settings	All VDA versions

Profile Management/Folder Redirection/Contacts

Name	Default setting	VDA
Contacts path	Disabled. No location is specified.	All VDA versions
Redirection settings for Contacts	Contents are redirected to the UNC path specified in the Contacts path policy settings	All VDA versions

Profile Management/Folder Redirection/Desktop

Name	Default setting	VDA
Desktop path	Disabled. No location is specified.	All VDA versions
Redirection settings for Desktop	Contents are redirected to the UNC path specified in the Desktop path policy settings	All VDA versions

Profile Management/Folder Redirection/Documents

Name	Default setting	VDA
Documents path	Disabled. No location is specified.	All VDA versions
Redirection settings for Documents	Contents are redirected to the UNC path specified in the Documents path policy settings	All VDA versions

Profile Management/Folder Redirection/Downloads

Name	Default setting	VDA
Downloads path	Disabled. No location is specified.	All VDA versions
Redirection settings for Downloads	Contents are redirected to the UNC path specified in the Downloads path policy settings	All VDA versions

Profile Management/Folder Redirection/Favorites

Name	Default setting	VDA
Favorites path	Disabled. No location is specified.	All VDA versions
Redirection settings for Favorites	Contents are redirected to the UNC path specified in the Favorites path policy settings	All VDA versions

Profile Management/Folder Redirection/Links

Name	Default setting	VDA
Links path	Disabled. No location is specified.	All VDA versions
Redirection settings for Links	Contents are redirected to the UNC path specified in the Links path policy settings	All VDA versions

Profile Management/Folder Redirection/Music

Name	Default setting	VDA
Music path	Disabled. No location is specified.	All VDA versions
Redirection settings for Music	Contents are redirected to the UNC path specified in the Music path policy settings	All VDA versions

Profile Management/Folder Redirection/Pictures

Name	Default setting	VDA
Pictures path	Disabled. No location is specified.	All VDA versions
Redirection settings for Pictures	Contents are redirected to the UNC path specified in the Pictures path policy settings	All VDA versions

Name	Default setting	VDA

Profile Management/Folder Redirection/Saved Games

Name	Default setting	VDA
Saved Games path	Disabled. No location is specified.	All VDA versions
Redirection settings for Saved Games	Contents are redirected to the UNC path specified in the Saved Games path policy settings	All VDA versions

Profile Management/Folder Redirection/Searches

Name	Default setting	VDA
Searches path	Disabled. No location is specified.	All VDA versions
Redirection settings for Searches	Contents are redirected to the UNC path specified in the Searches path policy settings	All VDA versions

Profile Management/Folder Redirection/Start Menu

Name	Default setting	VDA
Start Menu path	Disabled. No location is specified.	All VDA versions
Redirection settings for Start Menu	Contents are redirected to the UNC path specified in the Start Menu path policy settings	All VDA versions

Profile Management/Folder Redirection/Video

Name	Default setting	VDA
Video path	Disabled. No location is specified.	All VDA versions
Redirection settings for Video	Contents are redirected to the UNC path specified in the Video path policy settings	All VDA versions

Profile Management/Log settings

Name	Default setting	VDA
Active Directory actions	Disabled	All VDA versions
Common information	Disabled	All VDA

Name	Default setting	VDA versions
Common warnings	Disabled	All VDA versions
Enable logging	Disabled	All VDA versions
File system actions	Disabled	All VDA versions
File system notifications	Disabled	All VDA versions
Logoff	Disabled	All VDA versions
Logon	Disabled	All VDA versions
Maximum size of the log file	1048576	All VDA versions
Path to log file	Disabled. Log files are saved in the default location; %SystemRoot%\System32\Logfiles\UserProfileManager.	All VDA versions
Personalized user information	Disabled	All VDA versions
Policy values at logon and logoff	Disabled	All VDA versions
Registry actions	Disabled	All VDA versions
Registry differences at logoff	Disabled	All VDA versions

Profile Management/Profile handling

Name	Default setting	VDA
Delay before deleting cached profiles	0	All VDA versions
Delete locally cached profiles on logoff	Disabled	All VDA versions
Local profile conflict handling	Use local profile	All VDA versions

Name	Default setting	VDA
Migration of existing profiles	Local and roaming	All VDA versions
Path to the template profile	Disabled. New user profiles are created from the default user profile on the device where a user first logs on.	All VDA versions
Template profile overrides local profile	Disabled	All VDA versions
Template profile overrides roaming profile	Disabled	All VDA versions
Template profile used as a Citrix mandatory profile for all logons	Disabled	All VDA versions

Profile Management/Registry

Name	Default setting	VDA
Exclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions
Inclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions

Profile Management/Streamed user profiles

Name	Default setting	VDA
Always cache	Disabled	All VDA versions
Always cache size	0 Mb	All VDA versions
Profile streaming	Disabled	All VDA versions
Streamed user profile groups	Disabled. All user profiles within an OU are processed normally.	All VDA versions
Timeout for pending area lock files (days)	1 day	All VDA versions

Receiver

Name	Default setting	VDA
StoreFront	No stores are	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server

Name	Default setting	VDA
accounts list	specified	OS and VDA for Desktop OS

Virtual Delivery Agent

Name	Default setting	VDA
Controller registration IPv6 netmask	No netmask is specified	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Controller registration port	80	All VDA versions
Controller SIDs	No SIDs are specified	All VDA versions
Controllers	No controllers are specified	All VDA versions
Enable auto update of controllers	Enabled	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Only use IPv6 controller registration	Disabled	VDA for Server OS 7 and VDA for Desktop OS 7 through current VDA for Server OS and VDA for Desktop OS
Site GUID	No GUID is specified	All VDA versions

Virtual IP

Name	Default setting	VDA
Virtual IP loopback support	Disabled	VDA 7.6
Virtual IP virtual loopback programs list	None	VDA 7.6

HDX 3D Pro

Name	Default setting	VDA
Enable lossless	Enabled	VDA 5.5 and 5.6 Feature Pack 1
HDX 3D Pro quality settings		VDA 5.5 and 5.6 Feature Pack 1

Policy settings reference

Sep 29, 2015

Policies contain settings that are applied when the policy is enforced. Descriptions in this section also indicate if additional settings are required to enable a feature or are similar to a setting.

Quick reference

The following tables list the settings you can configure within a policy. Find the task you want to complete in the left column, then locate its corresponding setting in the right column.

Audio

For this task	Use this policy setting
Control whether to allow the use of multiple audio devices	Audio Plug N Play
Control whether to allow audio input from microphones on the user device	Client microphone redirection
Control audio quality on the user device	Audio quality
Control audio mapping to speakers on the user device	Client audio redirection

Bandwidth for user devices

To limit bandwidth used for	Use this policy setting
Client audio mapping	• Audio redirection bandwidth limit or • Audio redirection bandwidth limit percent
Cut-and-paste using local clipboard	• Clipboard redirection bandwidth limit or • Clipboard redirection bandwidth limit percent
Access in a session to local client drives	• File redirection bandwidth limit or • File redirection bandwidth limit percent
HDX MediaStream Multimedia Acceleration	• HDX MediaStream Multimedia Acceleration bandwidth limit or • HDX MediaStream Multimedia Acceleration bandwidth limit percent

To limit bandwidth used for	Use this policy setting
Client session	Overall session bandwidth limit
Printing	• Printer redirection bandwidth limit or • Printer redirection bandwidth limit percent
TWAIN devices (such as a camera or scanner)	• TWAIN device redirection bandwidth limit or • TWAIN device redirection bandwidth limit percent
USB devices	• Client USB device redirection bandwidth limit or • Client USB device redirection bandwidth limit percent

Redirection of client drives and user devices

For this task	Use this policy setting
Control whether or not drives on the user device are connected when users log on to the server	Auto connect client drives
Control cut-and-paste data transfer between the server and the local clipboard	Client clipboard redirection
Control how drives map from the user device	Client drive redirection
Control whether users' local hard drives are available in a session	• Client fixed drives and • Client drive redirection
Control whether users' local floppy drives are available in a session	• Client floppy drives and • Client drive redirection
Control whether users' network drives are available in a session	• Client network drives and • Client drive redirection
Control whether users' local CD, DVD, or Blu-ray drives are available in a session	• Client optical drives and • Client drive redirection
Control whether users' local removable drives are available in a session	• Client removable drives and • Client drive redirection
Control whether users' TWAIN devices, such as scanners and	• Client TWAIN device redirection

For this task	Use this policy setting
cameras, are available in a session and control compression of image data transfers	• TWAIN compression redirection
Control whether USB devices are available in a session	• Client USB device redirection and • Client USB device redirection rules
Improve the speed of writing and copying files to a client disk over a WAN	Use asynchronous writes

Content redirection

For this task	Use this policy setting
Control whether to use content redirection from the server to the user device	Host to client redirection

Desktop UI

For this task	Use this policy setting
Control whether or not Desktop wallpaper is used in users' sessions	Desktop wallpaper
View window contents while a window is dragged	View window contents while dragging

Graphics and multimedia

For this task	Use this policy setting
Control the maximum number of frames per second sent to user devices from virtual desktops	Target frame rate
Control the visual quality of images displayed on the user device	Visual quality
Control whether Flash content is rendered in sessions	Flash default behavior
Control whether websites can display Flash content when accessed in sessions	• Flash server-side content fetching URL list • Flash URL compatibility list

For this task	Use this policy setting
	• Flash video fallback prevention policy setting • Flash video fallback prevention error *.swf

Prioritize Multi-Stream network traffic

For this task	Use this policy setting
Specify ports for ICA traffic across multiple connections and establish network priorities	Multi-Port policy
Enable support for multi-stream connections between servers and user devices	Multi-Stream (computer and user settings)

Print

For this task	Use this policy setting
Control creation of client printers on the user device	• Auto-create client printers and • Client printer redirection
Control the location where printer properties are stored	Printer properties retention
Control whether print requests are processed by the client or the server	Direct connections to print servers
Control whether users can access printers connected to their user devices	Client printer redirection
Control installation of native Windows drivers when automatically creating client and network printers	Automatic installation of in-box printer drivers
Control when to use the Universal Printer Driver	Universal print driver usage
Choose a printer based on a roaming user's session information	Default printer

Note: Policies cannot be used to enable a screen saver in a desktop or application session. For users who require screen savers, the screen saver can be implemented on the user device.

ICA policy settings

Sep 29, 2015

The ICA section contains policy settings related to ICA listener connections and mapping to the clipboard.

Client clipboard redirection

This setting allows or prevents the clipboard on the user device being mapped to the clipboard on the server.

By default, clipboard redirection is allowed.

To prevent cut-and-paste data transfer between a session and the local clipboard, select Prohibit. Users can still cut and paste data between applications running in sessions.

After allowing this setting, configure the maximum allowed bandwidth the clipboard can consume in a client connection using the Clipboard redirection bandwidth limit or the Clipboard redirection bandwidth limit percent settings.

Client clipboard write allowed formats

When the Restrict client clipboard write setting is Enabled, host clipboard data cannot be shared with the client endpoint but you can use this setting to allow specific data formats to be shared with the client endpoint clipboard. To use this setting, enable it and add the specific formats to be allowed.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

The following custom formats are predefined in XenApp and XenDesktop:

- CFX_RICHTEXT

- CFX_OfficeDrawingShape
- CFX_BIFF8

Additional custom formats can be added. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if either Client clipboard redirection or Restrict client clipboard write is set to Prohibited.

Desktop launches

This setting allows or prevents non-administrative users in a VDA's Direct Access Users group connecting to a session on that VDA using an ICA connections.

By default, non-administrative users cannot connect to these sessions.

This setting has no effect on non-administrative users in a VDA's Direct Access Users group who are using a RDP connection; these users can connect to the VDA whether this setting is enabled or disabled. This setting has no effect on non-administrative users not in a VDA's Direct Access Users group; these users cannot connect to the VDA whether this setting is enabled or disabled.

ICA listener connection timeout

Note: This setting applies only to these Virtual Delivery Agents: 5.0, 5.5, and 5.6 Feature Pack 1.

This setting specifies the maximum wait time for a connection using the ICA protocol to be completed.

By default, the maximum wait time is 120000 milliseconds, or two minutes.

ICA listener port number

This setting specifies the TCP/IP port number used by the ICA protocol on the server.

By default, the port number is set to 1494.

Valid port numbers must be in the range of 0-65535 and must not conflict with other well-known port numbers. If you change the port number, restart the server for the new value to take effect. If you change the port number on the server, you must also change it on every Receiver or plug-in that connects to the server.

Launching of non-published programs during client connection

This setting specifies whether to allow launching initial applications through RDP on the server.

By default, launching initial applications through RDP on the server is not allowed.

Restrict client clipboard write

If this setting is Allowed, host clipboard data cannot be shared with the client endpoint. You can allow specific formats by enabling the Client clipboard write allowed formats setting.

By default, this is set to Prohibited.

Restrict session clipboard write

When this setting is Allowed, client clipboard data cannot be shared within the user session. You can allow specific formats by enabling the Session clipboard write allowed formats setting.

By default, this is set to Prohibited.

Session clipboard write allowed formats

When the Restrict session clipboard write setting is Allowed, client clipboard data cannot be shared with session applications, but you can use this setting to allow specific data formats to be shared with the session clipboard.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

The following custom formats are predefined in XenApp and XenDesktop:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Additional custom formats can be added. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if either the Client clipboard redirection setting or Restrict session clipboard write setting is set to Prohibited.

Auto Client Reconnect policy settings

Sep 29, 2015

The Auto Client Reconnect section contains policy settings for controlling the automatic reconnection of sessions.

Auto client reconnect

This setting allows or prevents automatic reconnection by the same client after a connection has been interrupted.

By default, automatic reconnection is allowed.

Allowing automatic reconnection allows users to resume working where they were interrupted when a connection was broken. Automatic reconnection detects broken connections and then reconnects the users to their sessions.

However, automatic reconnection can result in a new session being launched (instead of reconnecting to an existing session) if the Receiver's cookie, which contains the key to the session ID and credentials, is not used. The cookie is not used if it has expired, for example, because of a delay in reconnection, or if credentials must be reentered. Auto client reconnect is not triggered if users intentionally disconnect.

For application sessions, when automatic reconnection is allowed, Receiver attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For desktop sessions, when automatic reconnection is allowed, Receiver attempts to reconnect to the session for a specified period of time, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this period of time is five minutes. To change this period of time, edit this registry on the user device:

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>
where <seconds> is the number of seconds after which no more attempts are made to reconnect the session.

Auto client reconnect authentication

This setting requires authentication for automatic client reconnections.

By default, authentication is not required.

When a user initially logs on, their credentials are encrypted, stored in memory, and a cookie is created containing the encryption key that is sent to Receiver. When this setting is configured, cookies are not used. Instead, a dialog box is displayed to users requesting credentials when Receiver attempts to reconnect automatically.

Auto client reconnect logging

This setting enables or disables the recording of auto client reconnections in the event log.

By default, logging is disabled.

When logging is enabled, the server's System log captures information about successful and failed automatic reconnection events. A site does not provide a combined log of reconnection events for all servers.

Audio policy settings

Sep 30, 2014

The Audio section contains policy settings that permit user devices to send and receive audio in sessions without reducing performance.

Audio over UDP real-time transport

This setting allows or prevents the transmission and receipt of audio between the VDA and user device over RTP using the User Datagram Protocol (UDP). When this setting is disabled, audio is sent and received over TCP.

By default, audio over UDP is allowed.

Audio Plug N Play

This setting allows or prevents the use of multiple audio devices to record and play sound.

By default, the use of multiple audio devices is allowed.

This setting applies only to Windows Server OS machines.

Audio quality

This setting specifies the quality level of sound received in user sessions.

By default, sound quality is set to High - high definition audio.

To control sound quality, choose one of the following options:

- Select Low - for low speed connections for low-bandwidth connections. Sounds sent to the user device are compressed up to 16 Kbps. This compression results in a significant decrease in the quality of the sound but allows reasonable performance for a low-bandwidth connection.
- Select Medium - optimized for speech to deliver Voice over IP (VoIP) applications, to deliver media applications in challenging network connections with lines less than 512 Kbps, or significant congestion and packet loss. This codec offers very fast encode time, making it ideal for use with softphones and Unified Communications applications when you require server-side media processing.
  Audio sent to the user device is compressed up to 64 Kbps; this compression results in a moderate decrease in the quality of the audio played on the user device, while providing low latency and consuming low bandwidth. If VoIP quality is unsatisfactory, ensure that the Audio over UDP Real-time Transport policy setting is set to Allowed.
- Select High - high definition audio for connections where bandwidth is plentiful and sound quality is important. Clients can play sound at its native rate. Sounds are compressed at a high quality level maintaining up to CD quality, and using up to 112 Kbps of bandwidth. Transmitting this amount of data can result in increased CPU utilization and network congestion.

Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption is doubled.

To specify the maximum amount of bandwidth, configure the Audio redirection bandwidth limit or the Audio redirection bandwidth limit percent settings.

Client audio redirection

This setting specifies whether applications hosted on the server can play sounds through a sound device installed on the user device. This setting also specifies whether users can record audio input.

By default, audio redirection is allowed.

After allowing this setting, you can limit the bandwidth consumed by playing or recording audio. Limiting the amount of bandwidth consumed by audio can improve application performance but may also degrade audio quality. Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption doubles. To specify the maximum amount of bandwidth, configure the Audio redirection bandwidth limit or the Audio redirection bandwidth limit percent settings.

On Windows Server OS machines, ensure that the Audio Plug N Play setting is Enabled to support multiple audio devices.

Important: Prohibiting Client audio redirection disables all HDX audio functionality.

Client microphone redirection

This setting enables or disables client microphone redirection. When enabled, users can use microphones to record audio input in a session.

By default, microphone redirection is allowed.

For security, users are alerted when servers that are not trusted by their devices try to access microphones. Users can choose to accept or not accept access. Users can disable the alert on Citrix Receiver.

On Windows Server OS machines, ensure that the Audio Plug N Play setting is Enabled to support multiple audio devices.

If the Client audio redirection setting is disabled on the user device, this rule has no effect.

Bandwidth policy settings

Sep 25, 2014

The Bandwidth section contains policy settings to avoid performance problems related to client session bandwidth use. Important: Using these policy settings with the Multi-Stream policy settings may produce unexpected results. If you use Multi-Stream settings in a policy, ensure these bandwidth limit policy settings are not included.

Audio redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for playing or recording audio in a user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Audio redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

Audio redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth limit for playing or recording audio as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Audio redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

Client USB device redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for the redirection of USB devices to and from the client.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Client USB device redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

Client USB device redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for the redirection of USB devices to and from the client as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Client USB device redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

Clipboard redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for data transfer between a session and the local clipboard.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Clipboard redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

Clipboard redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for data transfer between a session and the local clipboard as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Clipboard redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

COM port redirection bandwidth limit

Note: For the Virtual Delivery Agent 7.x, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.
This setting specifies the maximum allowed bandwidth in kilobits per second for accessing a COM port in a client connection. If you enter a value for this setting and a value for the COM port redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

COM port redirection bandwidth limit percent

Note: For the Virtual Delivery Agent 7.x, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.
This setting specifies the maximum allowed bandwidth for accessing COM ports in a client connection as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified

If you enter a value for this setting and a value for the COM port redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions

File redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for accessing a client drive in a user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the File redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) takes effect.

File redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth limit for accessing client drives as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the File redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

HDX MediaStream Multimedia Acceleration bandwidth limit

This setting specifies the maximum allowed bandwidth limit, in kilobits per second, for delivering streaming audio and video using HDX MediaStream Multimedia Acceleration.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the HDX MediaStream Multimedia Acceleration bandwidth limit percent setting, the most restrictive setting (with the lower value) takes effect.

HDX MediaStream Multimedia Acceleration bandwidth limit percent

This setting specifies the maximum allowed bandwidth for delivering streaming audio and video using HDX MediaStream Multimedia Acceleration as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the HDX MediaStream Multimedia Acceleration bandwidth limit setting, the most restrictive setting (with the lower value) takes effect.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

LPT port redirection bandwidth limit

Note: For the Virtual Delivery Agent 7.x, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.
This setting specifies the maximum allowed bandwidth, in kilobits per second, for print jobs using an LPT port in a single user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the LPT port redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

LPT port redirection bandwidth limit percent

Note: For the Virtual Delivery Agent 7.x, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.
This setting specifies the bandwidth limit for print jobs using an LPT port in a single client session as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the LPT port redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

Overall session bandwidth limit

This setting specifies the total amount of bandwidth available, in kilobits per second, for user sessions.

The maximum enforceable bandwidth cap is 10 Mbps (10,000 Kbps). By default, no maximum (zero) is specified.

Limiting the amount of bandwidth consumed by a client connection can improve performance when other applications outside the client connection are competing for limited bandwidth.

Printer redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for accessing client printers in a user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Printer redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

Printer redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for accessing client printers as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Printer redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

TWAIN device redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for controlling TWAIN imaging devices from published applications.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the TWAIN device redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

TWAIN device redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for controlling TWAIN imaging devices from published applications as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the TWAIN device redirection bandwidth limit setting, the most

restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

Client sensors policy settings

Jul 24, 2014

The Client Sensors section contains policy settings for controlling how mobile device sensor information is handled in a user session.

Allow applications to use the physical location of the client device

This setting determines whether applications running in a session on a mobile device are allowed to use the physical location of the user device.

By default, the use of location information is prohibited

When this setting is prohibited, attempts by an application to retrieve location information return a "permission denied" value.

When this setting is allowed, a user can prohibit use of location information by denying a Receiver request to access the location. Android and iOS devices prompt at the first request for location information in each session.

When developing hosted applications that use the Allow applications to use the physical location of the client device setting, consider the following:

- A location-enabled application should not rely on location information being available because:
  - A user might not allow access to location information.
  - The location might not be available or might change while the application is running.
  - A user might connect to the application session from a different device that does not support location information.
- A location-enabled application must:
  - Have the location feature off by default.
  - Provide a user option to allow or disallow the feature while the application is running.
  - Provide a user option to clear location data that is cached by the application. (Receiver does not cache location data.)
- A location-enabled application must manage the granularity of the location information so that the data acquired is appropriate to the purpose of the application and conforms to regulations in all relevant jurisdictions.
- A secure connection (for example, using SSL/TLS or a VPN) should be enforced when using location services. Citrix Receiver should connect to trusted servers.
- Consider obtaining legal advice regarding the use of location services.

Desktop UI policy settings

Aug 08, 2016

The Desktop UI section contains policy settings that control visual effects such as desktop wallpaper, menu animations, and drag-and-drop images, to manage the bandwidth used in client connections. You can improve application performance on a WAN by limiting bandwidth usage.

Desktop Composition Redirection

This setting specifies whether to use the processing capabilities of the graphics processing unit (GPU) or integrated graphics processor (IGP) on the user device for local DirectX graphics rendering to provide users with a more fluid Windows desktop experience. When enabled, Desktop Composition Redirection delivers a highly responsive Windows experience while maintaining high scalability on the server.

By default, Desktop Composition Redirection is disabled (7.6 FP3 through current) and enabled (5.6 through 7.6 FP2).

To turn off Desktop Composition Redirection and reduce the bandwidth required in user sessions, select Disabled when adding this setting to a policy.

Desktop Composition Redirection graphics quality

This setting specifies the quality of graphics used for Desktop Composition Redirection.

By default, this is set to high.

Choose from High, Medium, Low, or Lossless quality.

Desktop wallpaper

This setting allows or prevents wallpaper showing in user sessions.

By default, user sessions can show wallpaper.

To turn off desktop wallpaper and reduce the bandwidth required in user sessions, select Prohibited when adding this setting to a policy.

Menu animation

This setting allows or prevents menu animation in user sessions.

By default, menu animation is allowed.

Menu animation is a Microsoft personal preference setting for ease of access. When enabled, it causes a menu to appear after a short delay, either by scrolling or fading in. An arrow icon appears at the bottom of the menu. The menu appears when you point to that arrow.

Menu animation is enabled on a desktop if this policy setting is set to Allowed and the menu animation Microsoft personal preference setting is enabled.

Note: Changes to the menu animation Microsoft personal preference setting are changes to the desktop. This means that if the desktop is set to discard changes when the session ends, a user who has enabled menu animations in a session may not have menu animation available in subsequent sessions on the desktop. For users who require menu animation, enable

the Microsoft setting in the master image for the desktop or ensure that the desktop retains user changes.

View window contents while dragging

This setting allows or prevents the display of window contents when dragging a window across the screen.

By default, viewing window contents is allowed.

When set to Allowed, the entire window appears to move when you drag it. When set to Prohibited, only the window outline appears to move until you drop it.

End user monitoring policy settings

Jul 24, 2014

The End User Monitoring section contains policy settings for measuring session traffic.

ICA round trip calculation

This setting determines whether ICA round trip calculations are performed for active connections.

By default, calculations for active connections are enabled.

By default, each ICA round trip measurement initiation is delayed until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

ICA round trip calculation interval

This setting specifies the frequency, in seconds, at which ICA round trip calculations are performed.

By default, ICA round trip is calculated every 15 seconds.

ICA round trip calculations for idle connections

This setting determines whether ICA round trip calculations are performed for idle connections.

By default, calculations are not performed for idle connections.

By default, each ICA round trip measurement initiation is delayed until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

Enhanced desktop experience policy setting

Jul 24, 2014

The Enhanced Desktop Experience policy setting sessions running on server operating systems to look like local Windows 7 desktops, providing users with an enhanced desktop experience.

By default, this setting is allowed.

If a user profile with Windows Classic theme already exists on the virtual desktop, enabling this policy does not provide an enhanced desktop experience for that user. If a user with a Windows 7 theme user profile logs on to a virtual desktop running Windows Server 2012 for which this policy is either not configured or disabled, that user sees an error message indicating failure to apply the theme.

In both cases, resetting the user profile resolves the issue.

If the policy changes from enabled to disabled on a virtual desktop with active user sessions, the look and feel of those sessions is inconsistent with both the Windows 7 and Windows Classic desktop experience. To avoid this, ensure you restart the virtual desktop after changing this policy setting. You must also delete any roaming profiles on the virtual desktop. Citrix also recommends deleting any other user profiles on the virtual desktop to avoid inconsistencies between profiles.

If you are using roaming user profiles in your environment, ensure the Enhanced Desktop Experience feature is enabled or disabled for all virtual desktops that share a profile.

Citrix does not recommend sharing roaming profiles between virtual desktops running server operating systems and client operating systems. Profiles for client and server operating systems differ and sharing roaming profiles across both types can lead to inconsistencies in profile properties when a user moves between the two.

File Redirection policy settings

Jul 24, 2014

The File Redirection section contains policy settings relating to client drive mapping and client drive optimization.

Auto connect client drives

This setting allows or prevents automatic connection of client drives when users log on.

By default, automatic connection is allowed.

When adding this setting to a policy, make sure to enable the settings for the drive types you want automatically connected. For example, to allow automatic connection of users' CD-ROM drives, configure this setting and the Client optical drives setting.

The following policy settings are related:

- Client drive redirection
- Client floppy drives
- Client optical drives
- Client fixed drives
- Client network drives
- Client removable drives

Client drive redirection

This setting enables or disables file redirection to and from drives on the user device.

By default, file redirection is enabled.

When enabled, users can save files to all their client drives. When disabled, all file redirection is prevented, regardless of the state of the individual file redirection settings such as Client floppy drives and Client network drives.

The following policy settings are related:

- Client floppy drives
- Client optical drives
- Client fixed drives
- Client network drives
- Client removable drives

Client fixed drives

This setting allows or prevents users from accessing or saving files to fixed drives on the user device.

By default, accessing client fixed drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client fixed drives are not mapped and users cannot access these drives manually, regardless of the state of the Client fixed drives setting.

To ensure fixed drives are automatically connected when users log on, configure the Auto connect client drives setting.

Client floppy drives

This setting allows or prevents users from accessing or saving files to floppy drives on the user device.

By default, accessing client floppy drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client floppy drives are not mapped and users cannot access these drives manually, regardless of the state of the Client floppy drives setting.

To ensure floppy drives are automatically connected when users log on, configure the Auto connect client drives setting.

Client network drives

This setting allows or prevents users from accessing and saving files to network (remote) drives through the user device.

By default, accessing client network drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client network drives are not mapped and users cannot access these drives manually, regardless of the state of the Client network drives setting.

To ensure network drives are automatically connected when users log on, configure the Auto connect client drives setting.

Client optical drives

This setting allows or prevents users from accessing or saving files to CD-ROM, DVD-ROM, and BD-ROM drives on the user device.

By default, accessing client optical drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client optical drives are not mapped and users cannot access these drives manually, regardless of the state of the Client optical drives setting.

To ensure optical drives are automatically connected when users log on, configure the Auto connect client drives setting.

Client removable drives

This setting allows or prevents users from accessing or saving files to USB drives on the user device.

By default, accessing client removable drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client removable drives are not mapped and users cannot access these drives manually, regardless of the state of the Client removable drives setting.

To ensure removable drives are automatically connected when users log on, configure the Auto connect client drives setting.

Host to client redirection

This setting enables or disables file type associations for URLs and some media content to be opened on the user device. When disabled, content opens on the server.

By default, file type association is disabled.

These URL types are opened locally when you enable this setting:

- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- Real Player and QuickTime (RTSP)
- Real Player and QuickTime (RTSPU)
- Legacy Real Player (PNM)
- Microsoft Media Server (MMS)

Preserve client drive letters

This setting enables or disables mapping of client drives to the same drive letter in the session.

By default, client drive letters are not preserved.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed.

Read-only client drive access

This setting allows or prevents users and applications from creating or modifying files or folders on mapped client drives.

By default, files and folders on mapped client drives can be modified.

If set to Enabled, files and folders are accessible with read-only permissions.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed.

Special folder redirection

This setting allows or prevents Citrix Receiver and Web Interface users to see their local Documents and Desktop special folders from a session.

By default, special folder redirection is allowed.

This setting prevents any objects filtered through a policy from having special folder redirection, regardless of settings that exist elsewhere. When this setting is prohibited, any related settings specified for StoreFront, Web Interface, or Citrix Receiver are ignored.

To define which users can have special folder redirection, select Allowed and include this setting in a policy filtered on the users you want to have this feature. This setting overrides all other special folder redirection settings.

Because special folder redirection must interact with the user device, policy settings that prevent users from accessing or saving files to their local hard drives also prevent special folder redirection from working.

When adding this setting to a policy, make sure the Client fixed drives setting is present and set to Allowed.

Use asynchronous writes

This setting enables or disables asynchronous disk writes.

By default, asynchronous writes are disabled.

Asynchronous disk writes can improve the speed of file transfers and writing to client disks over WANs, which are typically

characterized by relatively high bandwidth and high latency. However, if there is a connection or disk fault, the client file or files being written may end in an undefined state. If this happens, a pop-up window informs the user of the files affected. The user can then take remedial action such as restarting an interrupted file transfer on reconnection or when the disk fault is corrected.

Citrix recommends enabling asynchronous disk writes only for users who need remote connectivity with good file access speed and who can easily recover files or data lost in the event of connection or disk failure.

When adding this setting to a policy, make sure that the Client drive redirection setting is present and set to Allowed. If this setting is disabled, asynchronous writes will not occur.

Flash Redirection policy settings

Sep 29, 2015

The Flash Redirection section contains policy settings for handling Flash content in user sessions.

Flash acceleration

This setting enables or disables Flash content rendering on user devices instead of the server. By default, client-side Flash content rendering is enabled.

Note: This setting is used for legacy Flash redirection with the Citrix online plug-in 12.1.
When enabled, this setting reduces network and server load by rendering Flash content on the user device. Additionally, the Flash URL compatibility list setting forces Flash content from specific websites to be rendered on the server.

On the user device, the Enable HDX MediaStream for Flash on the user device setting must be enabled as well.

When this setting is disabled, Flash content from all websites, regardless of URL, is rendered on the server. To allow only certain websites to render Flash content on the user device, configure the Flash URL compatibility list setting.

Flash background color list

This setting enables you to set key colors for given URLs.

By default, no key colors are specified.

Key colors appear behind client-rendered Flash and help provide visible region detection. The key color specified should be rare; otherwise, visible region detection might not work properly.

Valid entries consist of a URL (with optional wildcards at the beginning or end) followed by a 24-bit RGB color hexadecimal code. For example: http://citrix.com 000003.

Ensure that the URL specified is the URL for the Flash content, which might be different from the URL of the website.

> **Warning**
>
> Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

On VDA machines running Windows 8 or Windows 2012, this setting might fail to set key colors for the URL. If this occurs, edit the registry on the VDA machine.

For 32-bit machines, use this registry setting:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

For 64-bit machines, use this registry setting:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

"ForceHDXFlashEnabled"=dword:00000001

Flash backwards compatibility

This setting enables or disables the use of original, legacy Flash redirection features with older versions of Citrix Receiver (formerly the Citrix online plug-in).

By default, this setting is enabled.

On the user device, the Enable HDX MediaStream for Flash on the user device setting must also be enabled.

Second generation Flash redirection features are enabled for use with Citrix Receiver 3.0. Legacy redirection features are supported for use with the Citrix online plug-in 12.1. To ensure second generation Flash redirection features are used, both the server and the user device must have second generation Flash redirection enabled. If legacy redirection is enabled on either the server or the user device, legacy redirection features are used.

Flash default behavior

This setting establishes the default behavior for second generation Flash acceleration.

By default, Flash acceleration is enabled.

To configure this setting, choose one of the following options:

- Enable Flash acceleration. Flash Redirection is used.
- Block Flash Player. Flash Redirection and server-side rendering are not used. The user cannot view any Flash content.
- Disable Flash acceleration. Flash Redirection is not used. The user can view server-side rendered Flash content if a version of Adobe Flash Player for Windows Internet Explorer compatible with the content is installed on the server.

This setting can be overridden for individual Web pages and Flash instances based on the configuration of the Flash URL compatibility list setting. Additionally, the user device must have the Enable HDX MediaStream for Flash on the user device setting enabled.

Flash event logging

This setting enables Flash events to be recorded in the Windows application event log.

By default, logging is allowed.

On computers running Windows 7 or Windows Vista, a Flash redirection-specific log appears in the Applications and Services Log node.

Flash intelligent fallback

This setting enables or disables automatic attempts to employ server-side rendering for Flash Player instances where client-side rendering is either unnecessary or provides a poor user experience.

By default, this setting is enabled.

Flash latency threshold

This setting specifies a threshold between 0-30 milliseconds to determine where Adobe Flash content is rendered.

By default, the threshold is 30 milliseconds.

During startup, HDX MediaStream for Flash measures the current latency between the server and user device. If the latency is under the threshold, HDX MediaStream for Flash is used to render Flash content on the user device. If the latency is above the threshold, the network server renders the content if an Adobe Flash player is available there.

When enabling this setting, make sure the Flash backwards compatibility setting is also present and set to Enabled.

Note: Applies only when using HDX MediaStream Flash redirection in Legacy mode.

Flash video fallback prevention

This setting specifies if and how "small" flash content is rendered and displayed to users.

By default, this setting is not configured.

To configure this setting, choose one of the following options:

- **Only small content.** Only intelligent fallback content will be rendered on the server; other Flash content will be replaced with an error *.swf.
- **Only small content with a supported client.** Only intelligent fallback content will be rendered on the server if the client is currently using Flash Redirection; other content will be replaced with an error *.swf.
- **No server side content.** All content on the server will be replaced with an error *swf.

To use this policy setting you should specify an error *.swf file. This error *.swf will replace any content that you do not want to be rendered on the VDA.

Flash video fallback prevention error *.swf

This setting specifies the URL of the error message which is displayed to users to replace Flash instances when the server load management policies are in use. For example:

    http://domainName.tld/sample/path/error.swf

Flash server-side content fetching URL list

This setting specifies websites whose Flash content can be downloaded to the server and then transferred to the user device for rendering.

By default, no sites are specified.

This setting is used when the user device does not have direct access to the Internet; the server provides that connection. Additionally, the user device must have the Enable server-side content fetching setting enabled.

Second generation Flash redirection includes a fallback to server-side content fetching for Flash .swf files. If the user device is unable to fetch Flash content from a Web site, and the Web site is specified in the Flash server-side content fetching URL list, server-side content fetching occurs automatically.

When adding URLs to the list:

- Add the URL of the Flash application instead of the top-level HTML page that initiates the Flash Player.
- Use an asterisk (*) at the beginning or end of the URL as a wildcard.
- Use a trailing wildcard to allow all child URLs (http://www.citrix.com/*).
- The prefixes http:// and https:// are used when present, but are not required for valid list entries.

Flash URL compatibility list

This setting specifies the rules which determine whether Flash content on certain websites is rendered on the user device, rendered on the server, or blocked from rendering.

By default, no rules are specified.

When adding URLs to the list:

- Prioritize the list with the most important URLs, actions, and rendering locations at the top.
- Use an asterisk (*) at the beginning or end of the URL as a wildcard.
- Use a trailing wildcard to refer to all child URLs (http://www.citrix.com/*).
- The prefixes http:// and https:// are used when present, but are not required for valid list entries.
- Add to this list websites whose Flash content does not render correctly on the user device and select either the Render on Server or Block options.

Graphics policy settings

Mar 03, 2015

The Graphics section contains policy settings for controlling how images are handled in user sessions.

Display memory limit

This setting specifies the maximum video buffer size in kilobytes for the session.

By default, the display memory limit is 65536 kilobytes.

For connections requiring more color depth and higher resolution, increase the limit. Calculate the maximum memory required using the equation:

Memory depth in bytes = (color-depth-in-bits-per-pixel) / 8) * (vertical-resolution-in-pixels) * (horizontal-resolution-in-pixels).

For example, with a color depth of 32, vertical resolution of 600, and a horizontal resolution of 800, the maximum memory required is (32 / 8) * (600) * (800) = 1920000 bytes, which yields a display memory limit of 1920 KB.

Color depths other than 32-bit are available only if the Legacy graphics mode policy setting is enabled.

HDX allocates only the amount of display memory needed for each session. So, if only some users require more than the default, there is no negative impact on scalability by increasing the display memory limit.

Display mode degrade preference

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting specifies whether color depth or resolution degrades first when the session display memory limit is reached.

By default, color depth is degraded first.

When the session memory limit is reached, you can reduce the quality of displayed images by choosing whether color depth or resolution is degraded first. When color depth is degraded first, displayed images use fewer colors. When resolution is degraded first, displayed images use fewer pixels per inch.

To notify users when either color depth or resolution are degraded, configure the Notify user when display mode is degraded setting.

Dynamic windows preview

This setting enables or disables the display of seamless windows in Flip, Flip 3D, Taskbar Preview, and Peek window preview modes.

Windows Aero preview option	Description
Taskbar Preview	When the user hovers over a window's taskbar icon, an image of that window appears above the taskbar.
Windows Peek	When the user hovers over a taskbar preview image, a full-sized image of the window appears on the screen.

Windows Aero preview option	Description
Flip	When the user presses ALT+TAB, small preview icons are shown for each open window.
Flip 3D	When the user presses TAB+Windows logo key, large images of the open windows cascade across the screen.

By default, this setting is enabled.

Image caching

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting enables or disables the caching and retrieving of sections of images in sessions. Caching images in sections and retrieving these sections when needed makes scrolling smoother, reduces the amount of data transmitted over the network, and reduces the processing required on the user device.

By default, the image caching setting is enabled.

Note: The image caching setting controls how images are cached and retrieved; it does not control whether images are cached. Images are cached if the Legacy graphics mode setting is enabled.

Legacy graphics mode

This setting disables the rich graphics experience, providing fallback to the legacy graphics experience to improve scalability over a WAN or mobile connection.

By default, this setting is disabled and users are provided with the rich graphics experience.

Maximum allowed color depth

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting specifies the maximum color depth allowed for a session.

By default, the maximum allowed color depth is 32 bits per pixel.

This setting applies only to ThinWire drivers and connections. It does not apply to VDAs that have a non-ThinWire driver as the primary display driver, such as VDAs that use a Windows Display Driver Model (WDDM) driver as the primary display driver. For Desktop OS VDAs using a WDDM driver as the primary display driver, such as Windows 8, this setting has no effect. For Windows Server OS VDAs using a WDDM driver, such as Windows Server 2012 R2, this setting might prevent users from connecting to the VDA.

Setting a high color depth requires more memory. To degrade color depth when the memory limit is reached, configure the Display mode degrade preference setting. When color depth is degraded, displayed images use fewer colors.

Notify user when display mode is degraded

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting displays a brief explanation to the user when the color depth or resolution is degraded.

By default, notifying users is disabled.

Queuing and tossing

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting discards queued images that are replaced by another image.

By default, queuing and tossing is enabled.

This improves response when graphics are sent to the user device. Configuring this setting can cause animations to become choppy because of dropped frames.

Caching policy settings

Jul 24, 2014

The Caching section contains policy settings that enable caching image data on user devices when client connections are limited in bandwidth.

Persistent cache threshold

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting caches bitmaps on the hard drive of the user device. This enables re-use of large, frequently-used images from previous sessions.

By default, the threshold is 3000000 bits per second.

The threshold value represents the point below which the Persistent Cache feature will take effect. For example, using the default value, bitmaps are cached on the hard drive of the user device when bandwidth falls below 3000000 bps.

Keep alive policy settings

Jul 24, 2014

The Keep Alive section contains policy settings for managing ICA keep-alive messages.

ICA keep alive timeout

This setting specifies the number of seconds between successive ICA keep-alive messages.

By default, the interval between keep-alive messages is 60 seconds.

Specify an interval between 1-3600 seconds in which to send ICA keep-alive messages. Do not configure this setting if your network monitoring software is responsible for closing inactive connections.

ICA keep alives

This setting enables or disables sending ICA keep-alive messages periodically.

By default, keep-alive messages are not sent.

Enabling this setting prevents broken connections from being disconnected. If the server detects no activity, this setting prevents Remote Desktop Services (RDS) from disconnecting the session. The server sends keep-alive messages every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

ICA keep-alive does not work if you are using session reliability. Configure ICA keep-alive only for connections that are not using Session Reliability.

Related policy settings: Session reliability connections.

Local App Access policy settings

Jul 24, 2014

The Local App Access section contains policy settings that manage the integration of users' locally-installed applications with hosted applications in a hosted desktop environment.

Allow local app access

This setting allows or prevents the integration of users' locally-installed applications with hosted applications within a hosted desktop environment.

When a user launches a locally-installed application, that application appears to run within their virtual desktop, even though it is actually running locally.

By default, local app access is prohibited.

URL redirection black list

This setting specifies websites that are redirected to and launched in the local Web browser. This might include websites requiring locale information, such as msn.com or newsgoogle.com, or websites containing rich media content that are better rendered on the user device.

By default, no sites are specified.

URL redirection white list

This setting specifies websites that are rendered in the environment in which they are launched.

By default, no sites are specified.

Mobile experience policy settings

Sep 29, 2015

The Mobile Experience section contains policy settings for handling the Citrix Mobility Pack.

Automatic keyboard display

This setting enables or disables the automatic display of the keyboard on mobile device screens.

By default, the automatic display of the keyboard is disabled.

Launch touch-optimized desktop

This setting is disabled and not available for Windows 10 machines.

This setting determines the overall Receiver interface behavior by allowing or prohibiting a touch-friendly interface that is optimized for tablet devices.

By default, a touch-friendly interface is used.

To use only the Windows interface, set this policy setting to Prohibited.

Remote the combo box

This setting determines the types of combo boxes you can display in sessions on mobile devices. To display the device-native combo box control, set this policy setting to Allowed. When this setting is allowed, a user can change a Receiver for iOS session setting to use the Windows combo box.

By default, the Remote the combo box feature is prohibited.

Multimedia policy settings

Sep 29, 2015

The Multimedia section contains policy settings for managing streaming audio and video in user sessions.

Limit video quality

This setting specifies the maximum video quality level allowed for an HDX connection. When configured, maximum video quality is limited to the specified value, ensuring that multimedia Quality of Service (QoS) is maintained within an environment.

By default, this setting is not configured.

To limit the maximum video quality level allowed, choose one of the following options:

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

Note: Playing multiple videos simultaneously on the same server consumes large amounts of resources and may impact server scalability.

Multimedia conferencing

This setting allows or prevents support for video conferencing applications.

By default, video conferencing support is allowed.

When adding this setting to a policy, make sure the Windows Media Redirection setting is present and set to Allowed.

When using multimedia conferencing, make sure the following conditions are met:

- Manufacturer-supplied drivers for the web cam used for multimedia conferencing must be installed.
- The web cam must be connected to the user device before initiating a video conferencing session. The server uses only one installed web cam at any given time. If multiple web cams are installed on the user device, the server attempts to use each web cam in succession until a video conferencing session is created successfully.

Optimization for Windows Media multimedia redirection over WAN

This setting enables real-time multimedia transcoding, allowing audio and video media streaming to mobile devices, and enhancing the user experience by improving how Windows Media content is delivered over a WAN.

By default, the delivery of Windows Media content over the WAN is optimized.

When adding this setting to a policy, make sure the Windows Media Redirection setting is present and set to Allowed.

When this setting is enabled, real-time multimedia transcoding is deployed automatically as needed to enable media streaming, providing a seamless user experience even in extreme network conditions.

Use GPU for optimizing Windows Media multimedia redirection over WAN

This setting enables real-time multimedia transcoding to be done in the Graphics Processing Unit (GPU) on the Virtual

Delivery Agent (VDA), to improve server scalability. GPU transcoding is available only if the VDA has a supported GPU for hardware acceleration. Otherwise, transcoding falls back to the CPU.

Note: GPU transcoding is supported only on NVIDIA GPUs.
By default, using the GPU on the VDA to optimize the delivery of Windows Media content over the WAN is prohibited.

When adding this setting to a policy, make sure the Windows Media Redirection and Optimization for Windows Media multimedia redirection over WAN settings are present and set to Allowed.

Video fallback prevention

Administrators can use the Video fallback prevention policy setting to specify the methods that will be attempted to deliver streamed content to users.

By default, this setting is not configured. This allows Client Side Fetching to RAVE to Server Side fallbacks.

To configure this setting, choose one of the following options:

- **Server Fetched - Server Rendered**. Allow Client Side Fetching to RAVE to Server Side fallbacks.
- **Server Fetched - Client Rendered**. Allow Client Side Fetching to RAVE fallback, however, block RAVE to Server Side Rendering fallback.
- **Client Fetched - Client Rendered**. Block Client Side Fetching to RAVE to Server Side Rendering fallbacks.

When the content does not play, the error message "Company has blocked video because of lack of resources" displays in the player window.

Windows Media client-side content fetching

This setting enables a user device to stream multimedia files directly from the source provider on the Internet or Intranet, rather than through the host server.

By default, the streaming of multimedia files to the user device direct from the source provider is allowed.

Allowing this setting improves network utilization and server scalability by moving any processing on the media from the host server to the user device. It also removes the requirement that an advanced multimedia framework such as Microsoft DirectShow or Media Foundation be installed on the user device; the user device requires only the ability to play a file from a URL

When adding this setting to a policy, make sure the Windows Media Redirection setting is present and set to Allowed. If this setting is disabled, the streaming of multimedia files to the user device direct from the source provider is also disabled.

Windows Media Redirection

This setting controls and optimizes the way servers deliver streaming audio and video to users.

By default, the delivery of streaming audio and video to users is allowed.

Allowing this setting increases the quality of audio and video rendered from the server to a level that compares with audio and video played locally on a user device. The server streams multimedia to the client in the original, compressed form and allows the user device to decompress and render the media.

Windows Media redirection optimizes multimedia files that are encoded with codecs that adhere to Microsoft DirectShow, DirectX Media Objects (DMO), and Media Foundation standards. To play back a given multimedia file, a codec compatible

with the encoding format of the multimedia file must be present on the user device.

By default, audio is disabled on Citrix Receiver. To allow users to run multimedia applications in ICA sessions, turn on audio or give users permission to turn on audio in their Receiver interface.

Select Prohibited only if playing media using Windows Media redirection appears worse than when rendered using basic ICA compression and regular audio. This is rare but can happen under low bandwidth conditions, for example, with media with a very low frequency of key frames.

Windows Media Redirection buffer size

This setting specifies a buffer size from 1 to 10 seconds for multimedia acceleration.

By default, the buffer size is 5 seconds.

Windows Media Redirection buffer size use

This setting enables or disables using the buffer size specified in the Windows Media Redirection buffer size setting.

By default, the buffer size specified is not used.

If this setting is disabled or if the Windows Media Redirection buffer size setting is not configured, the server uses the default buffer size value (5 seconds).

Multi-stream connections policy settings

Aug 08, 2014

The Multi-Stream Connections section contains policy settings for managing Quality of Service (QoS) prioritization for multiple ICA connections in a session.

Audio over UDP

This setting allows or prevents audio over UDP on the server.

By default, audio over UDP is allowed on the server.

When enabled, this setting opens a UDP port on the server to support all connections configured to use Audio over UDP Realtime Transport.

Audio UDP port range

This setting specifies the range of port numbers (in the form lowest port number,highest port number) used by the Virtual Delivery Agent (VDA) to exchange audio packet data with the user device. The VDA attempts to use each UDP port pair to exchange data with the user device, starting with the lowest and incrementing by two for each subsequent attempt. Each port handles both inbound and outbound traffic.

By default, this is set to 16500,16509.

Multi-Port policy

This setting specifies the TCP ports to be used for ICA traffic and establishes the network priority for each port.

By default, the primary port (2598) has a High priority.

When you configure ports, you can assign the following priorities:

- Very High - for real-time activities, such as webcam conferences
- High - for interactive elements, such as screen, keyboard, and mouse
- Medium - for bulk processes, such as client drive mapping
- Low - for background activities, such as printing

Each port must have a unique priority. For example, you cannot assign a Very High priority to both CGP port 1 and CGP port 3.

To remove a port from prioritization, set the port number to 0. You cannot remove the primary port and you cannot modify its priority level.

When configuring this setting, restart the server. This setting takes effect only when the Multi-Stream computer setting policy setting is enabled.

Multi-Stream computer setting

This setting enables or disables Multi-Stream on the server.

By default, Multi-Stream is disabled.

If you use Citrix Cloudbridge with Multi-Stream support in your environment, you do not need to configure this setting.

Configure this policy setting when using third-party routers or legacy Branch Repeaters to achieve the desired Quality of Service (QoS).

When configuring this setting, reboot the server to ensure changes take effect.
Important: Using this policy setting in conjunction with bandwidth limit policy settings such as Overall session bandwidth limit may produce unexpected results. When including this setting in a policy, ensure that bandwidth limit settings are not included.

Multi-Stream user setting

This setting enables or disables Multi-Stream on the user device.

By default, Multi-Stream is disabled for all users.

This setting takes effect only on hosts where the Multi-Stream computer setting policy setting is enabled.
Important: Using this policy setting with bandwidth limit policy settings such as Overall session bandwidth limit may produce unexpected results. When including this setting in a policy, ensure that bandwidth limit settings are not included.

Port redirection policy settings

Sep 15, 2014

The Port Redirection section contains policy settings for client LPT and COM port mapping.

Note: For the Virtual Delivery Agent 7.x, configure these settings using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.

Auto connect client COM ports

This setting enables or disables automatic connection of COM ports on user devices when users log on to a site.

By default, client COM ports are not automatically connected.

Auto connect client LPT ports

This setting enables or disables automatic connection of LPT ports on user devices when users log on to a site.

By default, client LPT ports are not connected automatically.

Client COM port redirection

This setting allows or prevents access to COM ports on the user device.

By default, COM port redirection is prohibited.

The following policy settings are related:

- COM port redirection bandwidth limit
- COM port redirection bandwidth limit percent

Client LPT port redirection

This setting allows or prevents access to LPT ports on the user device.

By default, LPT port redirection is prohibited.

LPT ports are used only by legacy applications that send print jobs to the LPT ports and not to the print objects on the user device. Most applications today can send print jobs to printer objects. This policy setting is necessary only for servers that host legacy applications that print to LPT ports.

The following policy settings are related:

- LPT port redirection bandwidth limit
- LPT port redirection bandwidth limit percent

Printing policy settings

Aug 26, 2014

The Printing section contains policy settings for managing client printing.

Client printer redirection

This setting controls whether client printers are mapped to a server when a user logs on to a session.

By default, client printer mapping is allowed. If this setting is disabled, the PDF printer for the session is not auto-created.

Related policy settings: auto-create client printers

Default printer

This setting specifies how the default printer on the user device is established in a session.

By default, the user's current printer is used as the default printer for the session.

To use the current Remote Desktop Services or Windows user profile setting for the default printer, select Do not adjust the user's default printer. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. The default printer in a session will be the first printer auto-created in the session, which is either:

- The first printer added locally to the Windows server in Control Panel > Devices and Printers.
- The first auto-created printer, if there are no printers added locally to the server.

You can use this option to present users with the nearest printer through profile settings (known as proximity printing).

Printer assignments

This setting provides an alternative to the Default printer and Session printers settings. Use the individual Default printer and Session printers settings to configure behaviors for a site, large group, or organizational unit. Use the Printer assignments setting to assign a large group of printers to multiple users.

This setting specifies how the default printer on the listed user devices is established in a session.

By default, the user's current printer is used as the default printer for the session.

It also specifies the network printers to be auto-created in a session for each user device. By default, no printers are specified.

- When setting the default printer value:
  To use the current default printer for the user device, select Do not adjust.

  To use the current Remote Desktop Services or Windows user profile setting for the default printer, select Do no adjust. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. The default printer in a session will be the first printer auto-created in the session, which is either:

  - The first printer added locally to the Windows server in Control Panel > Devices and Printers.
  - The first auto-created printer, if there are no printers added locally to the server.
- When setting the session printers value: to add printers, type the UNC path of the printer you want to auto-create.

After adding the printer, you can apply customized settings for the current session at every logon.

Printer auto-creation event log preference

This setting specifies the events that are logged during the printer auto-creation process. You can choose to log no errors or warnings, only errors, or errors and warnings.

By default, errors and warnings are logged.

An example of a warning is an event in which a printer's native driver could not be installed and the Universal print driver is installed instead. To use the Universal print driver in this scenario, configure the Universal print driver usage setting to Use universal printing only or Use universal printing only if requested driver is unavailable.

Session printers

This setting specifies the network printers to be auto-created in a session.

By default, no printers are specified.

To add printers, type the UNC path of the printer you want to auto-create. After adding the printer, you can apply customized settings for the current session at every logon.

Wait for printers to be created (server desktop)

This setting allows or prevents a delay in connecting to a session so that server desktop printers can be auto-created.

By default, a connection delay does not occur.

Client printers policy settings

Sep 29, 2015

The Client Printers section contains policy settings for client printers, including settings to autocreate client printers, retain printer properties, and connect to print servers.

Auto-create client printers

This setting specifies the client printers that are auto-created. This setting overrides default client printer auto-creation settings.

By default, all client printers are auto-created.

This setting takes effect only if the Client printer redirection setting is present and set to Allowed.

When adding this setting to a policy, select an option:

- Auto-create all client printers automatically creates all printers on a user device.
- Auto-create the client's default printer only automatically creates only the printer selected as the default printer on the user device.
- Auto-create local (non-network) client printers only automatically creates only printers directly connected to the user device through an LPT, COM, USB, TCP/IP, or other local port.
- Do not auto-create client printers turns off autocreation for all client printers when users log on. This causes the Remote Desktop Services (RDS) settings for autocreating client printers to override this setting in lower priority policies.

Auto-create generic universal printer

Note: Hotfixes that address the issues with this policy setting are available as Knowledge Center articles CTX141565 and CTX141566.

This setting enables or disables autocreation of the generic Citrix Universal Printer object for sessions where a user device compatible with Universal Printing is in use.

By default, the generic Universal Printer object is not autocreated.

The following policy settings are related:

- Universal print driver usage
- Universal driver preference

Client printer names

This setting selects the naming convention for auto-created client printers.

By default, standard printer names are used.

Select Standard printer names to use printer names such as "HPLaserJet 4 from clientname in session 3."

Select Legacy printer names to use old-style client printer names and preserve backward compatibility for users or groups using MetaFrame Presentation Server 3.0 or earlier. An example of a legacy printer name is "Client/clientname#/HPLaserJet 4." This option is less secure.

Note: This option is provided only for backwards compatibility with legacy versions of XenApp and XenDesktop.

Direct connections to print servers

This setting enables or disables direct connections from the virtual desktop or server hosting applications to a print server for client printers hosted on an accessible network share.

By default, direct connections are enabled.

Enable direct connections if the network print server is not across a WAN from the virtual desktop or server hosting applications. Direct communication results in faster printing if the network print server and the virtual desktop or server hosting applications are on the same LAN.

Disable direct connections if the network is across a WAN or has substantial latency or limited bandwidth. Print jobs are routed through the user device where they are redirected to the network print server. Data sent to the user device is compressed, so less bandwidth is consumed as the data travels across the WAN.

If two network printers have the same name, the printer on the same network as the user device is used.

Printer driver mapping and compatibility

This setting specifies the driver substitution rules for auto-created client printers.

By default, no rules are specified.

When you define driver substitution rules, you can allow or prevent printers to be created with the specified driver. Additionally, you can allow created printers to use only universal print drivers. Driver substitution overrides or maps printer driver names the user device provides, substituting an equivalent driver on the server. This gives server applications access to client printers that have the same drivers as the server, but different driver names.

You can add a driver mapping, edit an existing mapping, override custom settings for a mapping, remove a mapping, or change the order of driver entries in the list. When adding a mapping, enter the client printer driver name and then select the server driver you want to substitute.

Printer properties retention

This setting specifies whether or not to store printer properties and where to store them.

By default, the system determines if printer properties are stored on the user device, if available, or in the user profile.

When adding this setting to a policy, select an option:

- Saved on the client device only is for user devices that have a mandatory or roaming profile that is not saved. Choose this option only if all the servers in your farm are running XenApp 5 and above and your users are using Citrix online plug-in versions 9 through 12.x, or Citrix Receiver 3.x.
- Retained in user profile only is for user devices constrained by bandwidth (this option reduces network traffic) and logon speed or for users with legacy plug-ins. This option stores printer properties in the user profile on the server and prevents any properties exchange with the user device. Use this option with MetaFrame Presentation Server 3.0 or earlier and MetaFrame Presentation Server Client 8.x or earlier. Note that this is applicable only if a Remote Desktop Services (RDS) roaming profile is used.
- Held in profile only if not saved on client allows the system to determine where printer properties are stored. Printer properties are stored either on the user device, if available, or in the user profile. Although this option is the most flexible, it can also slow logon time and use extra bandwidth for system-checking.
- Do not retain printer properties prevents storing printer properties.

Retained and restored client printers

This setting enables or disables the retention and re-creation of printers on the user device. By default, client printers are auto-retained and auto-restored.

Retained printers are user-created printers that are created again, or remembered, at the start of the next session. When XenApp recreates a retained printer, it considers all policy settings except the Auto-create client printers setting.

Restored printers are printers fully customized by an administrator, with a saved state that is permanently attached to a client port.

Drivers policy settings

Jul 24, 2014

The Drivers section contains policy settings related to printer drivers.

Automatic installation of in-box printer drivers

This setting enables or disables the automatic installation of printer drivers from the Windows in-box driver set or from driver packages staged on the host using pnputil.exe /a.

By default, these drivers are installed as needed.

Universal driver preference

This setting specifies the order in which universal printer drivers are used, beginning with the first entry in the list.

By default, the preference order is:

- EMF
- XPS
- PCL5c
- PCL4
- PS

You can add, edit, or remove drivers, and change the order of drivers in the list.

Universal print driver usage

This setting specifies when to use universal printing.

By default, universal printing is used only if the requested driver is unavailable.

Universal printing employs generic printer drivers instead of standard model-specific drivers, potentially simplifying the burden of driver management on host computers. The availability of universal print drivers depends on the capabilities of the user device, host, and print server software. In certain configurations, universal printing might not be available.

When adding this setting to a policy, select an option:

- Use only printer model specific drivers specifies that the client printer uses only the standard model-specific drivers that are auto-created at logon. If the requested driver is unavailable, the client printer cannot be auto-created.
- Use universal printing only specifies that no standard model-specific drivers are used. Only universal print drivers are used to create printers.
- Use universal printing only if requested driver is unavailable uses standard model-specific drivers for printer creation if they are available. If the driver is not available on the server, the client printer is created automatically with the appropriate universal driver.
- Use printer model specific drivers only if universal printing is unavailable uses the universal print driver if it is available. If the driver is not available on the server, the client printer is created automatically with the appropriate model-specific printer driver.

Universal Print Server policy settings

Sep 29, 2015

The Universal Print Server section contains policy settings for handling the Universal Print Server.

Universal Print Server enable

This setting enables or disables the Universal Print Server feature on the virtual desktop or the server hosting applications. Apply this policy setting to Organizational Units (OUs) containing the virtual desktop or server hosting applications.

By default, the Universal Print Server is disabled.

When adding this setting to a policy, select one of the following options:

- **Enabled with fallback to Windows native remote printing**. Network printer connections are serviced by the Universal Print Server, if possible. If the Universal Print Server is not available, the Windows Print Provider is used. The Windows Print Provider continues to handle all printers previously created with the Windows Print Provider.
- **Enabled with no fallback to Windows native remote printing**. Network printer connections are serviced by the Universal Print Server exclusively. If the Universal Print Server is unavailable, the network printer connection fails. This setting effectively disables network printing through the Windows Print Provider. Printers previously created with the Windows Print Provider are not created while a policy containing this setting is active.
- **Disabled**. The Universal Print Server feature is disabled. No attempt is made to connect with the Universal Print Server when connecting to a network printer with a UNC name. Connections to remote printers continue to use the Windows native remote printing facility.

Universal Print Server print data stream (CGP) port

This setting specifies the TCP port number used by the Universal Print Server print data stream Common Gateway Protocol (CGP) listener. Apply this policy setting only to OUs containing the print server.

By default, the port number is set to 7229.

Valid port numbers must be in the range of 1 to 65535.

Universal Print Server print stream input bandwidth limit (kpbs)

This setting specifies the upper boundary (in kilobits per second) for the transfer rate of print data delivered from each print job to the Universal Print Server using CGP. Apply this policy setting to OUs containing the virtual desktop or server hosting applications.

By default, the value is 0, which specifies no upper boundary.

Universal Print Server web service (HTTP/SOAP) port

This setting specifies the TCP port number used by the Universal Print Server's web service (HTTP/SOAP) listener. The Universal Print Server is an optional component that enables the use of Citrix universal print drivers for network printing scenarios. When the Universal Print Server is used, printing commands are sent from XenApp and XenDesktop hosts to the Universal Print Server via SOAP over HTTP. This setting modifies the default TCP port on which the Universal Print Server listens for incoming HTTP/SOAP requests.

You must configure both host and print server HTTP port identically. If you do not configure the ports identically, the host software will not connect to the Universal Print Server. This setting changes the VDA on XenApp and XenDesktop. In

addition, you must change the default port on the Universal Print Server.

By default, the port number is set to 8080.

Valid port numbers must be in the range of 0 to 65535.

Universal printing policy settings

Jul 24, 2014

The Universal Printing section contains policy settings for managing universal printing.

Universal printing EMF processing mode

This setting controls the method of processing the EMF spool file on the Windows user device.

By default, EMF records are spooled directly to the printer.

When adding this setting to a policy, select an option:

- Reprocess EMFs for printer forces the EMF spool file to be reprocessed and sent through the GDI subsystem on the user device. You can use this setting for drivers that require EMF reprocessing but that might not be selected automatically in a session.
- Spool directly to printer, when used with the Citrix Universal print driver, ensures the EMF records are spooled and delivered to the user device for processing. Typically, these EMF spool files are injected directly to the client's spool queue. For printers and drivers that are compatible with the EMF format, this is the fastest printing method.

Universal printing image compression limit

This setting specifies the maximum quality and the minimum compression level available for images printed with the Citrix Universal print driver.

By default, the image compression limit is set to Best quality (lossless compression).

If No Compression is selected, compression is disabled for EMF printing only.

When adding this setting to a policy, select an option:

- No compression
- Best quality (lossless compression)
- High quality
- Standard quality
- Reduced quality (maximum compression)

When adding this setting to a policy that includes the Universal printing optimization defaults setting, be aware of the following:

- If the compression level in the Universal printing image compression limit setting is lower than the level defined in the Universal printing optimization defaults setting, images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

Universal printing optimization defaults

This setting specifies the default values for printing optimization when the universal print driver is created for a session.

- Desired image quality specifies the default image compression limit applied to universal printing. By default, Standard Quality is enabled, meaning that users can only print images using standard or reduced quality compression.
- Enable heavyweight compression enables or disables reducing bandwidth beyond the compression level set by Desired image quality, without losing image quality. By default, heavyweight compression is disabled.

- Image and Font Caching settings specify whether or not to cache images and fonts that appear multiple times in the print stream, ensuring each unique image or font is sent to the printer only once. By default, embedded images and fonts are cached. Note that these settings apply only if the user device supports this behavior.
- Allow non-administrators to modify these settings specifies whether or not users can change the default print optimization settings within a session. By default, users are not allowed to change the default print optimization settings.

Note: All of these options are supported for EMF printing. For XPS printing, only the Desired image quality option is supported.
When adding this setting to a policy that includes the Universal printing image compression limit setting, be aware of the following:
- If the compression level in the Universal printing image compression limit setting is lower than the level defined in the Universal printing optimization defaults setting, images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

Universal printing preview preference

This setting specifies whether or not to use the print preview function for auto-created or generic universal printers.

By default, print preview is not used for auto-created or generic universal printers.

When adding this setting to a policy, select an option:
- Do not use print preview for auto-created or generic universal printers
- Use print preview for auto-created printers only
- Use print preview for generic universal printers only
- Use print preview for both auto-created and generic universal printers

Universal printing print quality limit

This setting specifies the maximum dots per inch (dpi) available for generating printed output in a session.

By default, No Limit is enabled, meaning users can select the maximum print quality allowed by the printer to which they connect.

If this setting is configured, it limits the maximum print quality available to users in terms of output resolution. Both the print quality itself and the print quality capabilities of the printer to which the user connects are restricted to the configured setting. For example, if configured to Medium Resolution (600 DPI), users are restricted to printing output with a maximum quality of 600 DPI and the Print Quality setting on the Advanced tab of the Universal Printer dialog box shows resolution settings only up to and including Medium Quality (600 DPI).

When adding this setting to a policy, select an option:
- Draft (150 DPI)
- Low Resolution (300 DPI)
- Medium Resolution (600 DPI)
- High Resolution (1200 DPI)
- No Limit

Security policy settings

Apr 22, 2015

The Security section contains the policy setting for configuring session encryption and encryption of logon data.

SecureICA minimum encryption level

This setting specifies the minimum level at which to encrypt session data sent between the server and a user device.

Important:
For the Virtual Delivery Agent 7.x, this policy setting can be used only to enable the encryption of the logon data with RC5 128-bit encryption. Other settings are provided only for backwards compatibility with legacy versions of XenApp and XenDesktop.

For the VDA 7.x, encryption of session data is set using the basic settings of the VDA's Delivery group. If Enable Secure ICA is selected for the Delivery group, session data is encrypted with RC5 (128 bit) encryption. If Enable Secure ICA is not selected for the Delivery group, session data is encrypted with Basic encryption.
When adding this setting to a policy, select an option:

- Basic encrypts the client connection using a non-RC5 algorithm. It protects the data stream from being read directly, but it can be decrypted. By default, the server uses Basic encryption for client-server traffic.
- RC5 (128 bit) logon only encrypts the logon data with RC5 128-bit encryption and the client connection using Basic encryption.
- RC5 (40 bit) encrypts the client connection with RC5 40-bit encryption.
- RC5 (56 bit) encrypts the client connection with RC5 56-bit encryption.
- RC5 (128 bit) encrypts the client connection with RC5 128-bit encryption.

The settings you specify for client-server encryption can interact with any other encryption settings in your environment and your Windows operating system. If a higher priority encryption level is set on either a server or user device, settings you specify for published resources can be overridden.

You can raise encryption levels to further secure communications and message integrity for certain users. If a policy requires a higher encryption level, Receivers using a lower encryption level are denied connection.

SecureICA does not perform authentication or check data integrity. To provide end-to-end encryption for your site, use SecureICA with SSL/TLS encryption.

SecureICA does not use FIPS-compliant algorithms. If this is an issue, configure the server and Receivers to avoid using SecureICA.

Server limits policy settings

Sep 01, 2015

The Server Limits section contains the policy setting for controlling idle connections.

Server idle timer interval

This setting determines, in milliseconds, how long an uninterrupted user session is maintained if there is no input from the user.

By default, idle connections are not disconnected (server idle timer interval = 0).

> ### Note
>
> When this policy setting is used, an "Idle timer expired" dialog box might appear to users when the session has been idle for the specified time. This is a Mircosoft dialog box that is not controlled by Citirx policy settings. For more information, see http://support.citrix.com/article/CTX118618.

Session limits policy settings

Jul 24, 2014

The Session Limits section contains policy settings that control how long sessions remain connected before they are forced to log off.

Disconnected session timer

This setting enables or disables a timer that specifies how long a disconnected, locked desktop can remain locked before the session is logged off.

By default, disconnected sessions are not logged off.

Disconnected session timer interval

This setting specifies how many minutes a disconnected, locked desktop can remain locked before the session is logged off.

By default, the time period is 1440 minutes (24 hours).

Session connection timer

This setting enables or disables a timer that specifies the maximum duration of an uninterrupted connection between a user device and a desktop.

By default, this timer is disabled.

Session connection timer interval

This setting specifies the maximum number of minutes for an uninterrupted connection between a user device and a desktop.

By default, the maximum duration is 1440 minutes (24 hours).

Session idle timer

This setting enables or disables a timer that specifies how long an uninterrupted user device connection to a desktop will be maintained if there is no input from the user.

By default, this timer is enabled.

Session idle timer interval

This setting specifies how many minutes an uninterrupted user device connection to a desktop will be maintained if there is no input from the user.

By default, idle connections are maintained for 1440 minutes (24 hours).

Session reliability policy settings

Jul 24, 2014

The Session Reliability section contains policy settings for managing session reliability connections.

Session reliability connections

This setting allows or prevents sessions to remain open during a loss of network connectivity.

By default, session reliability is allowed.

Session reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes.

With session reliability, the session remains active on the server. To indicate that connectivity is lost, the user's display freezes and the cursor changes to a spinning hourglass until connectivity is restored. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session reliability reconnects users without reauthentication prompts. If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, configure the Auto client reconnect authentication setting to require authentication. Users are then prompted to reauthenticate when reconnecting to interrupted sessions.

If you use both session reliability and auto client reconnect, the two features work in sequence. Session reliability closes (or disconnects) the user session after the amount of time specified in the Session reliability timeout setting. After that, the auto client reconnect settings take effect, attempting to reconnect the user to the disconnected session.

Session reliability port number

This setting specifies the TCP port number for incoming session reliability connections.

By default, the port number is set to 2598.

Session reliability timeout

This setting specifies the length of time, in seconds, the session reliability proxy waits for a user to reconnect before allowing the session to be disconnected.

By default, this is set to 180 seconds, or three minutes.

Although you can extend the amount of time a session is kept open, this feature is designed to be convenient to the user and it does not prompt the user for reauthentication. As you extend the amount of time a session is kept open, chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.

Time zone control policy settings

Jul 24, 2014

The Time Zone Control section contains policy settings related to using local time in sessions.

Estimate local time for legacy clients

This setting enables or disables estimating the local time zone of user devices that send inaccurate time zone information to the server.

By default, the server estimates the local time zone when necessary.

This setting is intended for use with legacy receivers or ICA clients that do not send detailed time zone information to the server. When used with receivers that send detailed time zone information to the server, such as supported versions of Receiver for Windows, this setting has no effect.

Use local time of client

This setting determines the time zone setting of the user session. This can be either the time zone of the user session or the time zone of the user device.

By default, the time zone of the user session is used.

For this setting to take effect, enable the Allow time zone redirection setting in the Group Policy Editor (User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection).

TWAIN devices policy settings

Jul 24, 2014

The TWAIN devices section contains policy settings related to mapping client TWAIN devices, such as digital cameras or scanners, and optimizing image transfers from server to client.

> **Note**
>
> TWAIN 2.0 is not currently supported.

Client TWAIN device redirection

This setting allows or prevents users from accessing TWAIN devices on the user device from image processing applications hosted on servers. By default, TWAIN device redirection is allowed.

The following policy settings are related:

- TWAIN compression level
- TWAIN device redirection bandwidth limit
- TWAIN device redirection bandwidth limit percent

TWAIN compression level

This setting specifies the level of compression of image transfers from client to server. Use Low for best image quality, Medium for good image quality, or High for low image quality. By default, medium compression is applied.

USB devices policy settings

Jul 24, 2014

The USB devices section contains policy settings for managing file redirection for USB devices.

Client USB device optimization rules

In XenApp and XenDesktop 7.6 FP3, the Client USB device optimization rules can be applied to devices to disable optimization, or to change the optimization mode.

When a user plugs in a USB input device, the host checks if the device is allowed by the USB policy settings. If the device is allowed, the host then checks the **Client USB device optimization rules** for the device. If no rule is specified, then the device is handled as Interactive mode (02). Capture mode (04) is the recommended mode for signature devices. See descriptions below for available modes.

Good to know

- For the use of Wacom signature pads and tablets, we recommend that you disable the screen saver. Steps on how to do this are at the end of this section.
- Support for the optimization of Wacom STU signature pads and tablets series of products has been preconfigured in the installation of XenApp and XenDesktop policies for XenApp and XenDesktop 7.6 FP3.
- Signature devices work across XenApp and XenDesktop and do not require a driver to be used as a signature device. Wacom has additional software that can be installed to customize the device further. See http://www.wacom.com/.
- Drawing tablets. Certain drawing input devices may present as an HID device on PCI/ACPI buses and are not supported. These devices should be attached on a USB host controller on the client to be redirected inside a XenDesktop session.

Policy rules take the format of tag=value expressions separated by whitespace. The following tags are supported:

Tag Name	Description
Mode	The optimization mode is supported for input devices for class=**03**. Supported modes are: No optimization - value **01**. Interactive mode - value **02**. Recommended for devices such as pen tablets and 3D Pro mice. Capture mode - value **04**. Preferred for devices such as signature pads.
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor

Class	Class from either the device descriptor or an interface descriptor
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

Examples

Mode=00000004 VID=1230 PID=1230 class=03 #Input device operating in capture mode

Mode=00000002 VID=1230 PID=1230 class=03 #Input device operating in interactive mode (default)

Mode=00000001 VID=1230 PID=1230 class=03 #Input device operating without any optimization

Mode=00000100 VID=1230 PID=1230 # Device setup optimization disabled (default)

Mode=00000200 VID=1230 PID=1230 # Device setup optimization enabled

Disabling the optimization mode using a registry setting

The optimization mode can be disabled system-wide by a registry flag:

HKLM\System\CurrentControlSet\Services\Icausbb\Parameters

DisableInputOptimization DWORD - set value to **1**

A system restart is required for this registry change to take effect.

Disabling the screen saver for Wacom signature pad devices

For the use of Wacom signature pads and tablets, we recommend that you disable the screen saver as follows:

1. Install the **Wacom-STU-Driver** after redirecting the device.
2. Install **Wacom-STU-Display MSI** to gain access to the signature pad control panel.
3. Go to **Control Panel > Wacom STU Display > STU430** or **STU530**, and select the tab for your model.
4. Click **Change**, then select **Yes** when the UAC security window pops up.
5. Select **Disable slideshow**, then **Apply**.

Once the setting is set for one signature pad model, it is applied to all models.

Client USB device redirection

This setting allows or prevents redirection of USB devices to and from the user device.

By default, USB devices are not redirected.

Client USB device redirection rules

This setting specifies redirection rules for USB devices.

By default, no rules are specified.

When a user plugs in a USB device, the host device checks it against each policy rule in turn until a match is found. The first

match for any device is considered definitive. If the first match is an Allow rule, the device is remoted to the virtual desktop. If the first match is a Deny rule, the device is available only to the local desktop. If no match is found, default rules are used.

Policy rules take the format {Allow:|Deny:} followed by a set of tag= value expressions separated by whitespace. The following tags are supported:

Tag Name	Description
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating new policy rules, remember:

- Rules are case-insensitive.
- Rules may have an optional comment at the end, introduced by #.
- Blank and pure comment lines are ignored.
- Tags must use the matching operator = (for example, VID=1230_.
- Each rule must start on a new line or form part of a semicolon-separated list.
- Refer to the USB class codes available from the USB Implementers Forum, Inc. web site.

Examples of administrator-defined USB policy rules:

- Allow: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive
- Deny: Class=08 subclass=05 # Mass Storage
- To create a rule that denies all USB devices, use "DENY:" with no other tags.

Client USB plug and play device redirection

This setting allows or prevents plug-and-play devices such as cameras or point-of-sale (POS) devices to be used in a client session.

By default, plug-and-play device redirection is allowed. When set to Allowed, all plug-and-play devices for a specific user or group are redirected. When set to Prohibited, no devices are redirected.

Visual display policy settings

Sep 29, 2015

The Visual Display section contains policy settings for controlling the quality of images sent from virtual desktops to the user device.

Preferred color depth for simple graphics

Applies to XenApp and XenDesktop **7.6 FP3** only.

Allows lowering of the color depth at which simple graphics are set to **16 bits per pixel**, potentially improving responsiveness over low bandwidth connections, at the cost of a slight degradation of image quality. This option is supported only when a video codec is not used to compress graphics.

By default, this is set to 24 bits per pixel.

Target frame rate

This setting specifies the maximum number of frames per second sent from the virtual desktop to the user device.

By default, the maximum is 30 frames per second.

Setting a high number of frames per second (for example, 30) improves the user experience, but requires more bandwidth. Decreasing the number of frames per second (for example, 10) maximizes server scalability at the expense of user experience. For user devices with slower CPUs, specify a lower value to improve the user experience.

Use video codec for compression

Applies to XenApp and XenDesktop **7.6 FP3** only.

Allows use of a video codec to compress graphics when video decoding is available on the endpoint. When video decoding is not available on the endpoint, or when you specify **Do not use video codec** a combination of still image compression and bitmap caching is used.

By default, this is set to Use video codec when available.

Visual quality

This setting specifies the desired visual quality for images displayed on the user device.

By default, this is set to Medium.

To specify the quality of images, choose one of the following options:

- **Low**
- **Medium** - Offers the best performance and bandwidth efficiency in most use cases
- **High** - Recommended if you require visually lossless image quality
- **Build to lossless** - Sends lossy images to the user device during periods of high network activity and lossless images after network activity reduces; this setting improves performance over bandwidth-constrained network connections
- **Always lossless** - In cases where preserving image data is vital (for example, when displaying X-ray images where no loss of quality is acceptable), select Always lossless to ensure lossy data is never sent to the user device.

If the **Legacy graphics mode** setting is enabled, the **Visual quality** setting has no effect in the policy.

Moving images policy settings

Sep 29, 2015

The Moving Images section contains settings that enable you to remove or alter compression for dynamic images.

Minimum image quality

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting specifies the minimum acceptable image quality for Adaptive Display. The less compression used, the higher the quality of images displayed. Choose from Ultra High, Very High, High, Normal, or Low compression.

By default, this is set to Normal.

Moving image compression

This setting specifies whether or not Adaptive Display is enabled. Adaptive Display automatically adjusts the image quality of videos and transitional slides in slide shows based on available bandwidth. With Adaptive Display enabled, users should see smooth-running presentations with no reduction in quality.
By default, Adaptive Display is enabled.

For VDA versions 7.0 through 7.6, this setting applies only when Legacy graphics mode is enabled. For VDA versions 7.6 FP1, FP2 and FP3, this setting applies when Legacy graphics mode is enabled, or when the legacy graphics mode is disabled and a video codec is not used to compress graphics.

When legacy graphics mode is enabled, the session must be restarted before policy changes take effect. Adaptive Display is mutually exclusive with Progressive Display; enabling Adaptive Display disables Progressive Display and vice versa. However, both Progressive Display and Adaptive Display can be disabled at the same time. Progressive Display, as a legacy feature, is not recommended for XenApp or XenDesktop. Setting Progressive threshold Level will disable Adaptive Display.

Progressive compression level

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting provides a less detailed but faster initial display of images.

By default, no progressive compression is applied.

The more detailed image, defined by the normal lossy compression setting, appears when it becomes available. Use Very High or Ultra High compression for improved viewing of bandwidth-intensive graphics such as photographs.

For progressive compression to be effective, its compression level must be higher than the Lossy compression level setting.
Note: The increased level of compression associated with progressive compression also enhances the interactivity of dynamic images over client connections. The quality of a dynamic image, such as a rotating three-dimensional model, is temporarily decreased until the image stops moving, at which time the normal lossy compression setting is applied.
The following policy settings are related:

- Progressive compression threshold value
- Progressive heavyweight compression

Progressive compression threshold value

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting represents the maximum bandwidth in kilobits per second for a connection to which progressive compression is applied. This is applied only to client connections under this bandwidth.

By default, the threshold value is 2147483647 kilobits per second.

The following policy settings are related:
- Progressive compression threshold value
- Progressive heavyweight compression

Target minimum frame rate

This setting specifies the minimum frame rate per second the system attempts to maintain, for dynamic images, under low bandwidth conditions.
By default, this is set to 10fps.

For VDA versions 7.0 through 7.6, this setting applies only when Legacy graphics mode is enabled. For VDA versions 7.6 FP1 through FP3, this setting applies when the Legacy graphics mode is disabled or enabled.

Still images policy settings

Sep 29, 2015

The Still Images section contains settings that enable you to remove or alter compression for static images.

Extra color compression

This setting enables or disables the use of extra color compression on images delivered over client connections that are limited in bandwidth, improving responsiveness by reducing the quality of displayed images.
By default, extra color compression is disabled.

When enabled, extra color compression is applied only when the client connection bandwidth is below the Extra color compression threshold value. When the client connection bandwidth is above the threshold value or Disabled is selected, extra color compression is not applied.

Extra color compression threshold

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting represents the maximum bandwidth in kilobits per second for a connection below which extra color compression is applied. If the client connection bandwidth drops below the set value, extra color compression, if enabled, is applied.

By default, the threshold value is 8192 kilobits per second.

Heavyweight compression

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting enables or disables reducing bandwidth beyond progressive compression without losing image quality by using a more advanced, but more CPU-intensive, graphical algorithm.

By default, heavyweight compression is disabled.

If enabled, heavyweight compression applies to all lossy compression settings. It is supported on Citrix Receiver but has no effect on other plug-ins.

The following policy settings are related:

- Progressive compression level
- Progressive compression threshold value

Lossy compression level

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting controls the degree of lossy compression used on images delivered over client connections that are limited in bandwidth. In such cases, displaying images without compression can be slow.

By default, medium compression is selected.

For improved responsiveness with bandwidth-intensive images, use high compression. Where preserving image data is vital;

for example, when displaying X-ray images where no loss of quality is acceptable, you may not want to use lossy compression.

Related policy setting: Lossy compression threshold value

Lossy compression threshold value

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.
This setting represents the maximum bandwidth in kilobits per second for a connection to which lossy compression is applied.

By default, the threshold value is 2147483647 kilobits per second.

Adding the Lossy compression level setting to a policy and including no specified threshold can improve the display speed of high-detail bitmaps, such as photographs, over a LAN.

Related policy setting: Lossy compression level

WebSockets policy settings

Jul 24, 2014

The WebSockets section contains policy settings for accessing virtual desktops and hosted applications with Receiver for HTML5. The WebSockets feature increases security and reduces overhead by conducting two-way communication between browser-based applications and servers without opening multiple HTTP connections.

WebSockets connections

This setting allows or prohibits WebSockets connections.

By default, WebSocket connections are prohibited.

WebSockets port number

This setting identifies the port for incoming WebSocket connections.

By default, the value is 8008.

WebSockets trusted origin server list

This setting provides a comma-separated list of trusted origin servers, usually Receiver for Web, expressed as URLs. Only WebSockets connections originating from one of these addresses is accepted by the server.

By default, the wildcard * is used to trust all Receiver for Web URLs.

If you choose to type an address in the list, use this syntax:

<protocol>://<Fully qualified domain name of host>:[port]

The protocol should be HTTP or HTTPS. If the port is not specified, port 80 is used for HTTP and port 443 is used for HTTPS.

The wildcard * can be used within the URL, except as part of an IP address (10.105.*.*).

Load management policy settings

Jul 24, 2014

The Load Management section contains policy settings for enabling and configuring load management between servers delivering Windows Server OS machines.

Concurrent logon tolerance

This setting specifies the maximum number of concurrent logons a server can accept.

By default, this is set to 2.

CPU usage

This setting specifies the level of CPU usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and CPU usage is excluded from load calculations.

CPU usage excluded process priority

This setting specifies the priority level at which a process' CPU usage is excluded from the CPU Usage load index.

By default, this is set to Below Normal or Low.

Disk usage

This setting specifies the disk queue length at which the server reports a 75% full load. When enabled, the default value for disk queue length is 8.

By default, this setting is disabled and disk usage is excluded from load calculations.

Maximum number of sessions

This setting specifies the maximum number of sessions a server can host. When enabled, the default setting for maximum number of sessions a server can host is 250.

By default, this setting is enabled.

Memory usage

This setting specifies the level of memory usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and memory usage is excluded from load calculations.

Memory usage base load

This setting specifies an approximation of the base operating system's memory usage and defines, in MB, the memory usage below which a server is considered to have zero load.

By default, this is set to 768 MB.

Profile management policy settings

Sep 15, 2016

The Profile Management section contains policy settings for enabling profile management and specifying which groups to include in and exclude from profile management processing.

Other information (such as the names of the equivalent .ini file settings and which version of profile management is required for a policy setting) is available in Profile Management Policies.

Advanced policy settings

Jul 25, 2014

The Advanced settings section contains policy settings relating to the advanced configuration of Profile management.

Disable automatic configuration

This setting enables profile management to examine your environment, for example, to check for the presence of Personal vDisks and configure Group Policy accordingly. Only Profile management policies in the Not Configured state are adjusted, so any customizations made previously are preserved. This feature speeds up deployment and simplifies optimization. No configuration of the feature is necessary, but you can disable automatic configuration when upgrading (to retain settings from earlier versions) or when troubleshooting. Automatic configuration does not work in XenApp or other environments.

By default, automatic configuration is allowed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, automatic configuration is turned on so Profile management settings might change if your environment changes.

Log off user if a problem is encountered

This setting enables Profile management to log a user off if a problem is encountered; for example, if the user store is unavailable. When enabled, an error message is displayed to the user before they are logged off. When disabled, users are given a temporary profile.

By default, this setting is disabled and users are given a temporary profile if a problem is encountered.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, a temporary profile is provided.

Number of retries when accessing locked files

This setting specifies the number of attempts Profile management makes to access locked files.

By default, this is set to five retries.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

Process Internet cookie files on logoff

This setting enables Profile management to process index.dat on logoff to remove Internet cookies left in the file system after sustained browsing that can lead to profile bloat. Enabling this setting increases logoff times, so only enable it if you experience this issue.

By default, this setting is disabled and Profile management does not process index.dat on logoff.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no processing of Index.dat takes place.

Basic policy settings

Jul 25, 2014

The Basic settings section contains policy settings relating to the basic configuration of Profile management.

Active write back

This setting enables modified files and folders (but not registry settings) to be synchronized to the user store during a session, before logoff.

By default, synchronization to the user store during a session is disabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is enabled.

Enable Profile management

This setting enables Profile management to process logons and logoffs.

By default, this is setting is disabled to facilitate deployment.

Important: Citrix recommends enabling Profile management only after carrying out all other setup tasks and testing how Citrix user profiles perform in your environment.
If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, Profile management does not process Windows user profiles in any way.

Excluded groups

This setting specifies which computer local groups and domain groups (local, global, and universal) are excluded from Profile management processing.

When enabled, Profile management does not process members of the specified user groups.

By default, this setting is disabled and members of all user groups are processed.

Specify domain groups in the form <DOMAIN NAME>\<GROUP NAME>.

If this setting is not configured here, the value from the .ini file is used .

If this setting is not configured here or in the .ini file, members of all user groups are processed.

Offline profile support

This setting enables offline profile support, allowing profiles to synchronize with the user store at the earliest opportunity after a network disconnection.

By default, support for offline profiles is disabled.

This setting is applicable to laptop or mobile users who roam. When a network disconnection occurs, profiles remain intact on the laptop or device even after restarting or hibernating. As mobile users work, their profiles are updated locally and are

synchronized with the user store when the network connection is re-established.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, support for offline profiles is disabled.

Path to user store

This setting specifies the path to the directory (user store) in which user settings, such as registry settings and synchronized files, are saved.

By default, the Windows directory on the home drive is used.

If this setting is disabled, user settings are saved in the Windows subdirectory of the home directory.

The path can be:

- **A relative path**.This must be relative to the home directory, typically configured as the #homeDirectory# attribute for a user in Active Directory.
- **An absolute UNC path**. This typically specifies a server share or a DFS namespace.
- **Disabled or unconfigured**. In this case, a value of #homeDirectory#\Windows is assumed.

Use the following types of variables when configuring this policy setting:

- System environment variables enclosed in percent signs (for example, %ProfVer%). Note that system environment variables generally require additional setup.
- Attributes of the Active Directory user object enclosed in hashes (for example, #sAMAccountName#).
- Profile management variables. For more information, see the Profile management documentation.

You can also use the %username% and %userdomain% user environment variables and create custom attributes to fully define organizational variables such as location or users. Attributes are case-sensitive.

Examples:

- \\server\share\#sAMAccountName# stores the user settings to the UNC path \\server\share\JohnSmith (if #sAMAccountName# resolves to JohnSmith for the current user)
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS! might expand to \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64

Important: Whichever attributes or variables you use, check that this setting expands to the folder one level higher than the folder containing NTUSER.DAT. For example, if this file is contained in \\server\profiles$\JohnSmith.Finance\v2x64\UPM_Profile, set the path to the user store as \\server\profiles$\JohnSmith.Finance\v2x64, not the \UPM_Profile subfolder.
If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the Windows directory on the home drive is used.

Process logons of local administrators

This setting specifies whether or not logons of members of the BUILTIN\Administrators group are processed. This allows domain users with local administrator rights, typically users with assigned virtual desktops, to bypass processing, log on, and troubleshoot a desktop experiencing problems with Profile management.

If this setting is disabled or not configured on server operating systems, Profile management assumes that logons by domain users, but not local administrators, must be processed. On desktop operating systems, local administrator logons

are processed.

By default this setting is disabled, and local administrator logons are not processed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, local administrator logons are not processed.

Processed groups

This setting specifies which computer local groups and domain groups (local, global, and universal) are included in Profile management processing.

When enabled, Profile management processes only members of the specified user groups.

By default, this setting is disabled and members of all user groups are processed.

Specify domain groups in the form <DOMAIN NAME>\<GROUP NAME>.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, members of all user groups are processed.

Cross-platform policy settings

Jul 25, 2014

The Cross-Platform section contains policy settings relating to configuring the Profile management cross-platform settings feature.

Cross-platform settings user groups

This setting specifies the Windows user groups whose profiles are processed when the cross-platform settings feature is enabled.

By default, this setting is disabled and all user groups specified in the Processed Group policy setting are processed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all user groups are processed.

Enable cross-platform settings

This setting enables or disables the cross-platforms settings feature, that allows you to migrate users' profiles and roam them when a user connects to the same application running on multiple operating systems.

By default the cross-platform settings feature is disabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no cross-platform settings are applied.

Path to cross-platform definitions

This setting specifies the network location, as a UNC path, of the definition files copied from the download package.

Note: Users must have read access, and administrators write access, to this location and it must be either a Server Message Block (SMB) or Common Internet File System (CIFS) file share.
By default, no path is specified.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no cross-platform settings are applied.

Path to cross-platform settings store

This setting specifies the path to the cross-settings store, the folder in which users' cross-platform settings are saved. This path can be either a UNC path or a path relative to the home directory.

Note: Users must have write access to the cross-settings store.
By default, this setting is disabled and the path Windows\PM_CP is used.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

Source for creating cross-platform settings

This setting specifies a platform as the base platform if this setting is enabled for that platform's OU. Data from the base platform's profiles is migrated to the cross-platform settings store.

Each platform's own set of profiles are stored in a separate OU. This means you must decide which platform's profile data to use to seed the cross-platform settings store. This is referred to as the base platform.

When enabled, Profile management migrates the data from the single-platform profile to the store if the cross-platform settings store contains a definition file with no data, or if the cached data in a single-platform profile is newer than the definition's data in the store.

Important: If this setting is enabled in multiple OUs, or multiple user or machine objects, the platform that the first user logs on to becomes the base profile.
By default, this setting is disabled and Profile management does not migrate the data from the single-platform profile to the store.

File system policy settings

Jul 25, 2014

The File System section contains policy settings for configuring which files and directories in a users profile are synchronized between the system where the profile is installed and the user store.

Exclusions policy settings

Jul 25, 2014

The Exclusions section contains policy settings for configuring which files and directories in a users profile are excluded from the synchronization process.

Exclusion list - directories

This setting specifies a list of folders in the user profile that are ignored during synchronization.

Specify folder names as paths relative to the user profile (%USERPROFILE%).

By default, this setting is disabled and all folders in the user profile are synchronized.

Example: Desktop ignores the Desktop folder in the user profile

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all folders in the user profile are synchronized.

Exclusion list - files

This setting specifies a list of files in the user profile that are ignored during synchronization.

By default, this setting is disabled and all files in the user profile are synchronized.

Specify file names as paths relative to the user profile (%USERPROFILE%). Note that wildcards are allowed and are applied recursively.

Example: Desktop\Desktop.ini ignores the file Desktop.ini in the Desktop folder

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all files in the user profile are synchronized.

Synchronization policy settings

Jan 18, 2016

The Synchronization section contains policy settings for specifying which files and folders in a users profile are synchronized between the system on which the profile is installed and the user store.

Directories to synchronize

This setting specifies any files you want Profile management to include in the synchronization process that are located in excluded folders. By default, Profile management synchronizes everything in the user profile. It is not necessary to include subfolders of the user profile by adding them to this list. For more information, see Include and exclude items.

Paths on this list must be relative to the user profile.

Example: Desktop\exclude\include ensures that the subfolder called include is synchronized even if the folder called Desktop\exclude is not

By default, this setting is disabled and no folders are specified.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, only non-excluded folders in the user profile are synchronized.

Files to synchronize

This setting specifies any files you want Profile management to include in the synchronization process that are located in excluded folders. By default, Profile management synchronizes everything in the user profile. It is not necessary to include files in the user profile by adding them to this list. For more information, see Include and exclude items.

Paths on this list must be relative to the user profile. Relative paths are interpreted as being relative to the user profile. Wildcards can be used but are allowed only for file names. Wildcards cannot be nested and are applied recursively.

Examples:

- AppData\Local\Microsoft\Office\Access.qat specifies a file below a folder that is excluded in the default configuration
- AppData\Local\MyApp*.cfg specifies all files with the extension .cfg in the profile folder AppData\Local\MyApp and its subfolders

By default, this setting is disabled and no files are specified.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, only non-excluded files in the user profile are synchronized.

Folders to mirror

This setting specifies which folders relative to a user's profile root folder to mirror. Configuring this policy setting can help solve issues involving any transactional folder (also known as a referential folder), that is a folder containing interdependent files, where one file references others.

Mirroring folders allows Profile management to process a transactional folder and its contents as a single entity, avoiding profile bloat. Be aware that, in these situations the "last write wins" so files in mirrored folders that have been modified in more than one session will be overwritten by the last update, resulting in loss of profile changes.

For example, you can mirror the Internet Explorer cookies folder so that Index.dat is synchronized with the cookies that it indexes.

If a user has two Internet Explorer sessions, each on a different server, and they visit different sites in each session, cookies from each site are added to the appropriate server. When the user logs off from the first session (or in the middle of a session, if the active write back feature is configured), the cookies from the second session should replace those from the first session. However, instead they are merged, and the references to the cookies in Index.dat become out of date. Further browsing in new sessions results in repeated merging and a bloated cookie folder.

Mirroring the cookie folder solves the issue by overwriting the cookies with those from the last session each time the user logs off so Index.dat stays up to date.

By default, this setting is disabled and no folders are mirrored.

If this setting is not configured here, the value from the .ini file is used.

If this policy is not configured here or in the .ini file, no folders are mirrored.

Folder redirection policy settings

Jul 25, 2014

The Folder Redirection section contains policy settings that specify whether to redirect folders that commonly appear in profiles to a shared network location.

Grant administrator access

This setting enables an administrator to access the contents of a user's redirected folders.

By default, this setting is disabled and users are granted exclusive access to the contents of their redirected folders.

Include domain name

This setting enables the inclusion of the %userdomain% environment variable as part of the UNC path specified for redirected folders.

By default, this setting is disabled and the %userdomain% environment variable is not included as part of the UNC path specified for redirected folders.

AppData(Roaming) policy settings

Jul 25, 2014

The AppData(Roaming) section contains policy settings for specifying whether to redirect the contents the AppData(Roaming) folder to a shared network location.

AppData(Roaming) path

This setting specifies the network location to which the contents of the AppData(Roaming) folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Redirection settings for AppData(Roaming)

This setting specifies how to redirect the contents of the AppData(Roaming) folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Contacts policy settings

Jul 25, 2014

The Contacts section contains policy settings for specifying whether to redirect the contents the Contacts folder to a shared network location.

Contacts path

This setting specifies the network location to which the contents of the Contacts folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Redirection settings for Contacts

This setting specifies how to redirect the contents of the Contacts folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Desktop policy settings

Jul 25, 2014

The Desktop section contains policy settings for specifying whether to redirect the contents the Desktop folder to a shared network location.

Desktop path

This setting specifies the network location to which the contents of the Desktop folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Redirection settings for Desktop

This setting specifies how to redirect the contents of the Desktop folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Documents policy settings

Mar 25, 2015

The Documents section contains policy settings for specifying whether to redirect the contents the Documents folder to a shared network location.

Documents path

This setting specifies the network location to which files in the Documents folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

The Documents path setting must be enabled not only to redirect files to the Documents folder, but also to redirect files to the Music, Pictures, and Videos folders.

Redirection settings for Documents

This setting specifies how to redirect the contents of the Documents folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Documents folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Documents path policy setting.
- Redirect to the users home directory. Redirects content to the users home directory, typically configured as the #homeDirectory# attribute for a user in Active Directory.

If this setting is not configured here, Profile management does not redirect the specified folder.

Downloads policy settings

Jul 25, 2014

The Downloads section contains policy settings that specify whether to redirect the contents the Downloads folder to a shared network location.

Downloads path

This setting specifies the network location to which files in the Downloads folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Redirection settings for Downloads

This setting specifies how to redirect the contents of the Downloads folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Favorites policy settings

Jul 25, 2014

The Favorites section contains policy settings that specify whether to redirect the contents the Favorites folder to a shared network location.

Favorites path

This setting specifies the network location to which the contents of the Favorites folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Redirection settings for Favorites

This setting specifies how to redirect the contents of the Favorites folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Links policy settings

Jul 25, 2014

The Links section contains policy settings that specify whether to redirect the contents the Links folder to a shared network location.

Links path

This setting specifies the network location to which the contents of the Links folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Redirection settings for Links

This setting specifies how to redirect the contents of the Links folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Music policy settings

Mar 25, 2015

The Music section contains policy settings that specify whether to redirect the contents the Music folder to a shared network location.

Music path

This setting specifies the network location to which the contents of the Music folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Redirection settings for Music

This setting specifies how to redirect the contents of the Music folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Music folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Music path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the Documents folder, the Documents path setting must be enabled.

If this setting is not configured here, Profile management does not redirect the specified folder.

Pictures policy settings

Mar 25, 2015

The Pictures section contains policy settings that specify whether to redirect the contents the Pictures folder to a shared network location.

Pictures path

This setting specifies the network location to which the contents of the Pictures folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Redirection settings for Pictures

This setting specifies how to redirect the contents of the Pictures folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Pictures folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Pictures path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the Documents folder, the Documents path setting must be enabled.

If this setting is not configured here, Profile management does not redirect the specified folder.

Saved Games policy settings

Jul 25, 2014

The Saved Games section contains policy settings that specify whether to redirect the contents the Saved Games folder to a shared network location.

Redirection settings for Saved Games

This setting specifies how to redirect the contents of the Saved Games folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Saved Games path

This setting specifies the network location to which the contents of the Saved Games folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Searches policy settings

Jul 25, 2014

The Searches section contains policy settings that specify whether to redirect the contents the Searches folder to a shared network location.

Redirection settings for Searches

This setting specifies how to redirect the contents of the Searches folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Searches path

This setting specifies the network location to which the contents of the Searches folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Start menu policy settings

Jul 25, 2014

The Start Menu section contains policy settings that specify whether to redirect the contents the Start Menu folder to a shared network location.

Redirection settings for Start Menu

This setting specifies how to redirect the contents of the Start Menu folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

Start Menu path

This setting specifies the network location to which the contents of the Start Menu folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Video policy settings

Mar 25, 2015

The Video section contains policy settings that specify whether to redirect the contents the Video folder to a shared network location.

Redirection settings for Video

This setting specifies how to redirect the contents of the Video folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Video folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Video path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the Documents folder, the Documents path setting must be enabled.

If this setting is not configured here, Profile management does not redirect the specified folder.

Video path

This setting specifies the network location to which the contents of the Video folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

Log policy settings

Jul 25, 2014

The Log section contains policy settings that configure Profile management logging.

Active Directory actions

This setting enables or disables verbose logging of actions performed in Active Directory.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Common information

This setting enables or disables verbose logging of common information.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Common warnings

This setting enables or disables verbose logging of common warnings.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Enable logging

This settings enables or disables Profile management logging in debug (verbose logging) mode. In debug mode, extensive status information is logged in the log files located in "%SystemRoot%\System32\Logfiles\UserProfileManager".

By default, this setting is disabled and only errors are logged.

Citrix recommends enabling this setting only if you are troubleshooting Profile management.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, only errors are logged.

File system actions

This setting enables or disables verbose logging of actions performed in the file system.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

File system notifications

This setting enables or disables verbose logging of file systems notifications.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Logoff

This setting enables or disables verbose logging of user logoffs.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Logon

This setting enables or disables verbose logging of user logons.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Maximum size of the log file

This setting specifies the maximum permitted size for the Profile management log file, in bytes.

By default, this is set to 1048576 bytes (1MB).

Citrix recommends increasing the size of this file to 5 MB or more, if you have sufficient disk space. If the log file grows beyond the maximum size, an existing backup of the file (.bak) is deleted, the log file is renamed to .bak, and a new log file is

created.

The log file is created in %SystemRoot%\System32\Logfiles\UserProfileManager.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

Path to log file

This setting specifies an alternative path to save the Profile management log file.

By default, this setting is disabled and log files are saved in the default location: %SystemRoot%\System32\Logfiles\UserProfileManager.

The path can point to a local drive or a remote network-based drive (UNC path). Remote paths can be useful in large distributed environments but they may create significant network traffic, which may be inappropriate for log files. For provisioned, virtual machines with a persistent hard drive, set a local path to that drive. This ensures log files are preserved when the machine restarts. For virtual machines without a persistent hard drive, setting a UNC path allows you to retain the log files, but the system account for the machines must have write access to the UNC share. Use a local path for any laptops managed by the offline profiles feature.

If a UNC path is used for log files, Citrix recommends that an appropriate access control list is applied to the log file folder to ensure that only authorized user or computer accounts can access the stored files.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default location %SystemRoot%\System32\Logfiles\UserProfileManager is used.

Personalized user information

This setting enables or disables verbose logging of personalized user information.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Policy values at logon and logoff

This setting enables or disables verbose logging of policy values when a user logs on and off.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Registry actions

This setting enables or disables verbose logging of actions performed in the registry.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Registry differences at logoff

This setting enables or disables verbose logging of any differences in the registry when a user logs off.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

Profile handling policy settings

Jul 25, 2014

The Profile handling section contains policy settings that specify how Profile management handles user profiles.

Delay before deleting cached profiles

This setting specifies an optional extension to the delay, in minutes, before Profile management deletes locally cached profiles at logoff.

A value of 0 deletes the profiles immediately at the end of the logoff process. Profile management checks for logoffs every minute, so a value of 60 ensures that profiles are deleted between one and two minutes after users log off (depending on when the last check occurred). Extending the delay is useful if you know that a process keeps files or the user registry hive open during logoff. With large profiles, this can also speed up logoff.

By default, this is set to 0 and Profile management deletes locally cached profiles immediately.

When enabling this setting, ensure the Delete locally cached profiles on logoff is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, profiles are deleted immediately.

Delete locally cached profiles on logoff

This setting specifies whether locally cached profiles are deleted after a user logs off.

When this setting is enabled, a user's local profile cache is deleted after they have logged off. Citrix recommends enabling this setting for terminal servers.

By default, this setting is disabled and a users local profile cache is retained after they log off.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, cached profiles are not deleted.

Local profile conflict handling

This setting configures how Profile management behaves if a user profile exists both in the user store and as a local Windows user profile (not a Citrix user profile).

By default, Profile management uses the local Windows profile, but does not change it in any way.

To control how Profile management behaves, choose one of the following options:

- Use local profile. Profile management uses the local profile, but does not change it in any way.
- Delete local profile. Profile management deletes the local Windows user profile, and then imports the Citrix user profile from the user store.
- Rename local profile. Profile management renames the local Windows user profile (for backup purposes) and then imports the Citrix user profile from the user store.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, existing local profiles are used.

Migration of existing profiles

This setting specifies the types of profile migrated to the user store during logon if a user has no current profile in the user store.

Profile management can migrate existing profiles "on the fly" during logon if a user has no profile in the user store. After this, the user store profile is used by Profile management in both the current session and any other session configured with the path to the same user store.

By default, both local and roaming profiles are migrated to the user store during logon.

To specifies the types of profile migrated to the user store during logon, choose one of the following options:

- Local and roaming profiles
- Local
- Roaming
- None (Disabled)

If you select None, the system uses the existing Windows mechanism to create new profiles, as if in a environment where Profile management is not installed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, existing local and roaming profiles are migrated.

Path to the template profile

This setting specifies the path to the profile you want Profile management to use as a template to create new user profiles.

The specified path must be the full path to the folder containing the NTUSER.DAT registry file and any other folders and files required for the template profile.
Note: Do not include NTUSER.DAT in the path. For example, with the file \\myservername\myprofiles\template\ntuser.dat, set the location as \\myservername\myprofiles\template.
Use absolute paths, which can be either UNC paths or paths on the local machine. Use the latter, for example, to specify a template profile permanently on a Citrix Provisioning Services image. Relative paths are not supported.

Note: This setting does not support expansion of Active Directory attributes, system environment variables, or the %USERNAME% and %USERDOMAIN% variables.
By default, this setting is disabled and new user profiles are created from the default user profile on the device where a user first logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Template profile overrides local profile

This setting enables the template profile to override the local profile when creating new user profiles.

If a user has no Citrix user profile, but a local Windows user profile exists, by default the local profile is used (and migrated to the user store, if this is not disabled). Enabling this policy setting allows the template profile to override the local profile used

when creating new user profiles.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Template profile overrides roaming profile

This setting enables the template profile to override a roaming profile when creating new user profiles.

If a user has no Citrix user profile, but a roaming Windows user profile exists, by default the roaming profile is used (and migrated to the user store, if this is not disabled). Enabling this policy setting allows the template profile to override the roaming profile used when creating new user profiles.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Template profile used as a Citrix mandatory profile for all logons

This setting enables Profile management to use the template profile as the default profile for creating all new user profiles.

By default, this setting is disabled and new user profiles are created from the default user profile on the device where a user first logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Registry policy settings

Jul 25, 2014

The Registry section contains policy settings that specify which registry keys are included or excluded from Profile management processing.

Exclusion list

This setting specifies the list of registry keys in the HKCU hive excluded from Profile management processing when a user logs off.

When enabled, keys specified in this list are excluded from processing when a user logs off.

By default, this setting is disabled, and all registry keys in the HKCU hive are processed when a user logs off.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no registry keys are excluded from processing.

Inclusion list

This setting specifies the list of registry keys in the HKCU hive included in Profile management processing when a user logs off.

When enabled, only keys specified in this list are processed when a user logs off.

By default, this setting is disabled, and all registry keys in the HKCU hive are processed when a user logs off.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all of HKCU is processed .

Streamed user profiles policy settings

Jul 25, 2014

The Streamed user profiles section contains policy settings that specify how Profile management processes streamed user profiles.

Always cache

This setting specifies whether or not Profile management caches streamed files as soon as possible after a user logs on. Caching files after a user logs on saves network bandwidth, enhancing the user experience.

Use this setting with the Profile streaming setting.

By default, this setting is disabled and streamed files are not cached as soon as possible after a user logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled.

Always cache size

This setting specifies a lower limit, in megabytes, on the size of files that are streamed. Profile management caches any files this size or larger as soon as possible after a user logs on.

By default, this is set to 0 (zero) and the cache entire profile feature is used. When the cache entire profile feature is enabled, Profile management fetches all profile contents in the user store, after a user logs on, as a background task.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled.

Profile streaming

This setting enables and disables the Citrix streamed user profiles feature. When enabled, files and folders contained in a profile are fetched from the user store to the local computer only when they are accessed by users after they have logged on. Registry entries and files in the pending area are fetched immediately.

By default, profile streaming is disabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled.

Streamed user profile groups

This setting specifies which user profiles within an OU are streamed, based on Windows user groups.

When enabled, only user profiles within the specified user groups are streamed. All other user profiles are processed normally.

By default, this setting is disabled and all user profiles within an OU are processed normally.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all user profiles are processed.

Timeout for pending area lock files

This setting specifies the number of days after which users' files are written back to the user store from the pending area, in the event that the user store remains locked when a server becomes unresponsive. This prevents bloat in the pending area and ensures the user store always contains the most up-to-date files.

By default, this is set to 1 (one) day.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

Receiver policy settings

Jul 25, 2014

The Receiver section contains policy settings that specify a list of StoreFront addresses to push to Receiver for Windows running on the virtual desktop.

StoreFront accounts list

This settings specifies a list of StoreFront stores administrators can choose to push to Receiver for Windows running on the virtual desktop. When creating a Delivery Group, administrators can select which stores to push to Receiver for Windows running on virtual desktops within that group.

By default, no stores are specified.

For each store, specify the following information as a semicolon-delimited entry:

- Store name. The name displayed to users of the store.
- Store URL. The URL for the store.
- Store enabled state. Whether or not the store is available to users. This is either On or Off.
- Store description. The description displayed to users of the store.

For example: Sales Store;https://sales.mycompany.com/Citrix/Store/discovery;On;Store for Sales staff

Virtual Delivery Agent policy settings

Jul 25, 2014

The Virtual Delivery Agent (VDA) section contains policy settings that control communication between the VDA and controllers for a site.

Important: The VDA requires information provided by these settings to register with a Delivery Controller, if you are not using the auto-update feature. Because this information is required for registration, you must configure the following settings using the Group Policy Editor, unless you provide this information during the VDA installation:

- Controller registration IPv6 netmask
- Controller registration port
- Controller SIDs
- Controllers
- Only use IPv6 controller registration
- Site GUID

Controller registration IPv6 netmask

This policy setting allows administrators to restrict the VDA to only a preferred subnet (rather than a global IP, if one is registered). This setting specifies the IPv6 address and network where the VDA will register. The VDA will register only on the first address that matches the specified netmask. This setting is valid only if the Only use IPv6 controller registration policy setting is enabled.

By default this setting is blank.

Controller registration port

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies the TCP/IP port number the VDA uses to register with a Controller when using registry-based registration.

By default, the port number is set to 80.

Controller SIDs

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies a space-separated list of controller Security Identifiers (SIDs) the VDA uses to register with a Controller when using registry-based registration. This is an optional setting which may be used with the Controllers setting to restrict the list of Controllers used for registration.

By default, this setting is blank.

Controllers

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies a space-separated list of controller Fully Qualified Domain Names (FQDNs) the VDA uses to register with a Controller when using registry-based registration. This is an optional setting that may be used with the Controller SIDs setting.

By default, this setting is blank.

Enable auto update of controllers

This setting enables the VDA to register with a Controller automatically after installation.

After the VDA registers, the Controller with which it registered sends a list of the current controller FQDNs and SIDs to the VDA. The VDA writes this list to persistent storage. Each Controller also checks the Site database every 90 minutes for Controller information; if a Controller has been added or removed since the last check, or if a policy change has occurred, the Controller sends updated lists to its registered VDAs. The VDA will accept connections from all the Controllers in the most recent list it received.

By default, this setting is enabled.

Only use IPv6 controller registration

This setting controls which form of address the VDA uses to register with the Controller:

- When enabled, the VDA registers with the Controller using the machine's IPv6 address. When the VDA communicates with the Controller, it uses the following address order: global IP address, Unique Local Address (ULA), link-local address (if no other IPv6 addresses are available).
- When disabled, the VDA registers and communicates with the Controller using the machine's IPv4 address.

By default, this is setting is disabled.

Site GUID

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies the Globally Unique Identifier (GUID) of the site the VDA uses to register with a Controller when using Active Directory-based registration.

By default, this setting is blank.

HDX 3D Pro policy settings

Jul 25, 2014

The HDX 3D Pro section contains policy settings for enabling and configuring the image quality configuration tool for users. The tool enables users to optimize use of available bandwidth by adjusting in real time the balance between image quality and responsiveness.

Enable lossless

This setting specifies whether or not users can enable and disable lossless compression using the image quality configuration tool. By default, users are not given the option to enable lossless compression.

When a user enables lossless compression, the image quality is automatically set to the maximum value available in the image configuration tool. By default, either GPU or CPU-based compression can be used, according to the capabilities of the user device and the host computer.

HDX 3D Pro quality settings

This setting specifies the minimum and maximum values that define the range of image quality adjustment available to users in the image quality configuration tool.

Specify image quality values of between 0 and 100, inclusive. The maximum value must be greater than or equal to the minimum value.

Virtual IP policy settings

Aug 06, 2014

The Virtual IP section contains policy settings that control whether sessions have their own virtual loopback address.

Virtual IP loopback support

When this setting is enabled, each session has its own virtual loopback address. When disabled, sessions do not have individual loopback addresses.

By default, this setting is disabled.

Virtual IP virtual loopback programs list

This setting specifies the application executables that can use virtual loopback addresses. When adding programs to the list, specify only the executable name; you do not need to specify the entire path.

By default, no executables are specified.

Configure COM Port and LPT Port Redirection settings using the registry

Jul 24, 2014

Policy settings for COM Port and LPT Port Redirection are located under HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated on the VDA image or machine.

To enable COM port and LPT port redirection, add new registry keys of type REG_DWORD, as follows:
Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Registry key	Description	Permitted values
AllowComPortRedirection	Allow or prohibit COM port redirection	1 (Allow) or 0 (Prohibit)
LimitComBw	Bandwidth limit for COM port redirection channel	Numeric value
LimitComBWPercent	Bandwidth limit for COM port redirection channel as a percentage of total session bandwidth	Numeric value between 0 and 100
AutoConnectClientComPorts	Automatically connect COM ports from the user device	1 (Allow) or 0 (Prohibit)
AllowLptPortRedirection	Allow or prohibit LPT port redirection	1 (Allow) or 0 (Prohibit)
LimitLptBw	Bandwidth limit for LPT port redirection channel	Numeric value
LimitLptBwPercent	Bandwidth limit for LPT port redirection channel as a percentage of total session bandwidth	Numeric value between 0 and 100
AutoConnectClientLptPorts	Automatically connect LPT ports from the user device	1 (Allow) or 0 (Prohibit)

After configuring these settings, modify your machine catalogs to use the new master image or updated physical machine. Desktops are updated with the new settings the next time users log off.

Connector for Configuration Manager 2012 policy settings

Jun 18, 2014

The Connector for Configuration Manager 2012 section contains policy settings for configuring the Citrix Connector 7.5 agent.

Important: Warning, logoff, and reboot message policies apply only to deployments to Server OS machine catalogs that are managed manually or by Provisioning Services. For those machine catalogs, the Connector service alerts users when there are pending application installs or software updates.
For catalogs managed by MCS, use Studio to notify users. For manually managed Desktop OS catalogs, use Configuration Manager to notify users. For Desktop OS catalogs managed by Provisioning Services, use Provisioning Services to notify users.

Advance warning frequency interval

This setting defines the interval between appearances of the advance warning message to users.

Intervals are set using the format ddd.hh:mm:ss, where:
- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the interval setting is 1 hour (01:00:00).

Advance warning message box body text

This setting contains the editable text of the message to users notifying them of upcoming software updates or maintenance that requires them to log off.

By default, the message is: {TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}

Advance warning message box title

This setting contains the editable text of the title bar of the advance warning message to users.

By default, the title is: Upcoming Maintenance

Advance warning time period

This setting defines how far before maintenance the advance warning message first appears.

The time is set using the format ddd.hh:mm:ss, where:
- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the setting is 16 hours (16:00:00), indicating that the first advance warning message appears approximately 16

hours before maintenance.

Final force logoff message box body text

This setting contains the editable text of the message alerting users that a forced logoff has begun.

By default, the message is: The server is currently going offline for maintenance

Final force logoff message box title

This setting contains the editable text of the title bar of the final force logoff message.

By default, the title is: Notification From IT Staff

Force logoff grace period

This setting defines the period of time between notifying users to log off and the implementation of the forced logoff to process the pending maintenance.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the force logoff grace period setting is 5 minutes (00:05:00).

Force logoff message box body text

This setting contains the editable text of the message telling users to save their work and log off prior to the start of a forced logoff.

By default, the message contains the following: {TIMESTAMP} Please save your work and log off. The server will go offline for maintenance in {TIMELEFT}

Force logoff message box title

This setting contains the editable text of the title bar of the force logoff message.

By default, the title is: Notification From IT Staff

Image-managed mode

The Connector agent automatically detects if it is running on a machine clone managed by Provisioning Services or MCS. The agent blocks Configuration Manager updates on image-managed clones and automatically installs the updates on the master image of the catalog.

After a master image is updated, use Studio to orchestrate the reboot of MCS catalog clones. The Connector Agent automatically orchestrates the reboot of PVS catalog clones during Configuration Manager maintenance windows. To override this behavior so that software is installed on catalog clones by Configuration Manager, change Image-managed mode to Disabled.

Reboot message box body text

This setting contains the editable text of the message notifying users when the server is about to be restarted.

By default, the message is: The server is currently going offline for maintenance

Regular time interval at which the agent task is to run

This setting determines how frequently the Citrix Connector agent task runs.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the regular time interval setting is 5 minutes (00:05:00).

Printing

Mar 02, 2016

Managing printers in your environment is a multistage process:

1. Become familiar with printing concepts, if you are not already.
2. Plan your printing architecture. This includes analyzing your business needs, your existing printing infrastructure, how your users and applications interact with printing today, and which printing management model best applies to your environment.
3. Configure your printing environment by selecting a printer provisioning method and then creating policies to deploy your printing design. Update policies when new employees or servers are added.
4. Test a pilot printing configuration before deploying it to users.
5. Maintain your Citrix printing environment by managing printer drivers and optimizing printing performance.
6. Troubleshoot issues that may arise.

Printing concepts

Before you begin planning your deployment, make sure that you understand these core concepts for printing:

- The types of printer provisioning available
- How print jobs are routed
- The basics of printer driver management

Printing concepts build on Windows printing concepts. To configure and successfully manage printing in your environment, you must understand how Windows network and client printing works and how this translates into printing behavior in this environment.

Print process

In this environment, all printing is initiated (by the user) on machines hosting applications. Print jobs are redirected through the network print server or user device to the printing device.

There is no persistent workspace for users of virtual desktops and applications. When a session ends the user's workspace is deleted, thus all settings need to be rebuilt at the beginning of each session. As a result, each time a user starts a new session, the system must rebuild the user's workspace.

When a user prints:

- Determines what printers to provide to the user. This is known as printer provisioning.
- Restores the user's printing preferences.
- Determines which printer is the default for the session.

You can customize how to perform these tasks by configuring options for printer provisioning, print job routing, printer property retention, and driver management. Be sure to evaluate how the various option settings might change the performance of printing in your environment and the user experience.

Printer provisioning

The process that makes printers available in a session is known as provisioning. Printer provisioning is typically handled dynamically. That is, the printers that appear in a session are not predetermined and stored. Instead, the printers are assembled, based on policies, as the session is built during log on and reconnection. As a result, the printers can change

according to policy, user location, and network changes, provided they are reflected in policies. Thus, users who roam to a different location might see changes to their workspace.

The system also monitors client-side printers and dynamically adjusts in-session auto-created printers based on additions, deletions, and changes to the client-side printers. This dynamic printer discovery benefits mobile users as they connect from various devices.

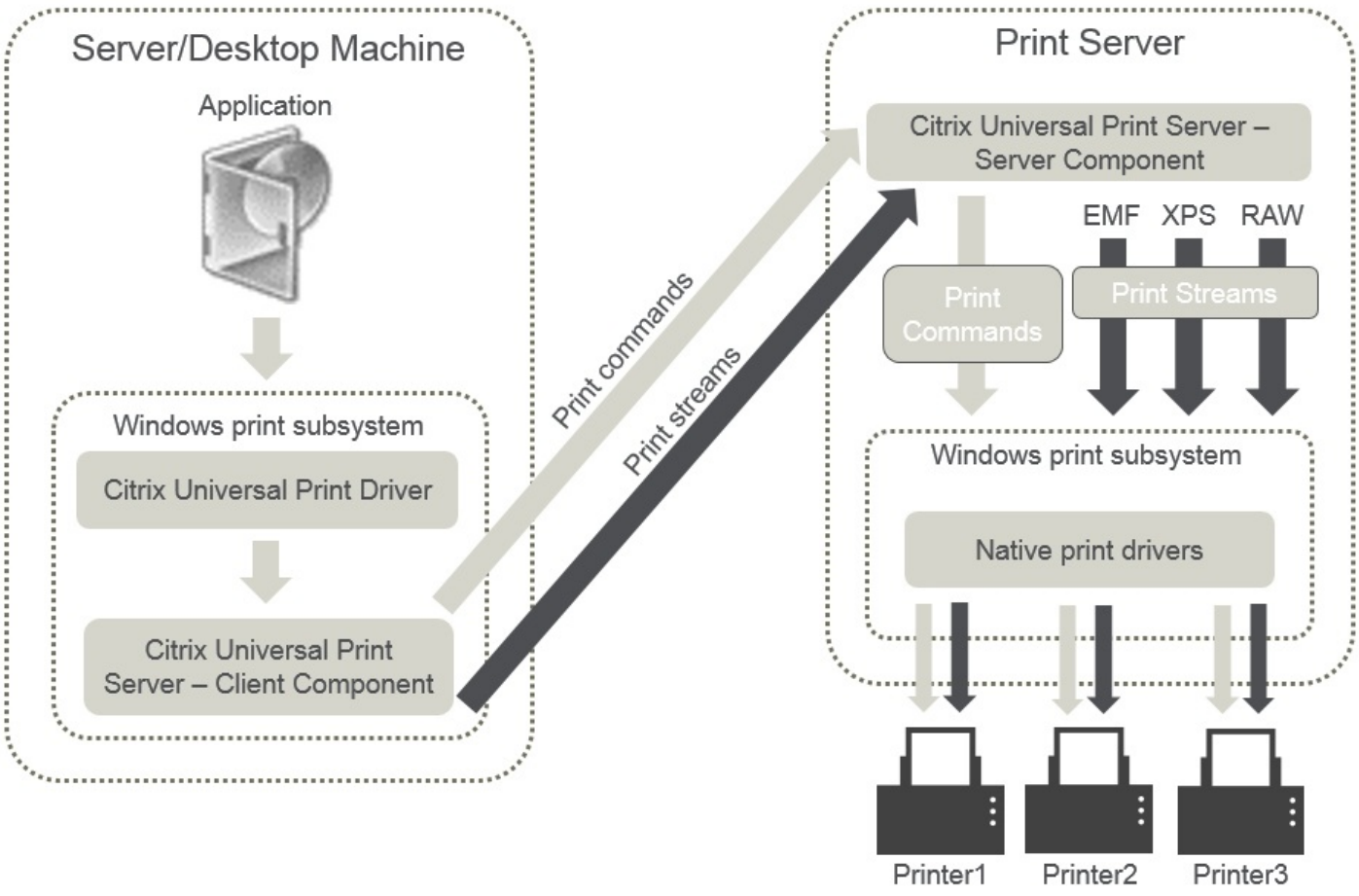
The most common methods of printer provisioning are:

- **Universal Print Server** - The Citrix Universal Print Server provides universal printing support for network printers. The Universal Print Server uses the Universal print driver. This solution enables you to use a single driver on a Server OS machine to allow network printing from any device.
  Citrix recommends the Citrix Universal Print Server for remote print server scenarios. The Universal Print Server transfers the print job over the network in an optimized and compressed format, thus minimizing network use and improving the user experience.

  The Universal Print Server feature comprises:
  - A client component, UPClient - Enable the UPClient on each Server OS machine that provisions session network printers and uses the Universal print driver.
  - A server component, UPServer - Install UPServer on each print server that provisions session network printers and uses the Universal print driver for the session printers (whether or not the session printers are centrally provisioned).

  For Universal Print Server requirements and setup details, refer to the system requirements and installation documents.

  Note: The Universal Print Server is also supported for VDI-in-a-Box 5.3. For information about installing Universal Print Server with VDI-in-a-Box, refer to the VDI-in-a-Box documentation.
  The following illustration shows the typical workflow for a network based printer in an environment that uses Universal Print Server.



When you enable the Citrix Universal Print Server, all connected network printers leverage it automatically through auto-discovery.

- **Autocreation** - *Autocreation* refers to printers automatically created at the beginning of each session. Both remote network printers and locally attached client printers can be auto-created. Consider auto-creating only the default client printer for environments with a large number of printers per user. Auto-creating a smaller number of printers uses less overhead (memory and CPU) on Server OS machines. Minimizing auto-created printers can also reduce user logon times. Auto-created printers are based on:

  - The printers installed on the user device.
  - Any policies that apply to the session.
    Autocreation policy settings enable you to limit the number or type of printers that are auto-created. By default, the printers are available in sessions when configuring all printers on the user device automatically, including locally attached and network printers.

  After the user ends the session, the printers for that session are deleted.

  Client and network printer autocreation has associated maintenance. For example, adding a printer requires that you:

  - Update the Session printers policy setting.
  - Add the driver to all Server OS machines using the Printer driver mapping and compatibility policy setting.

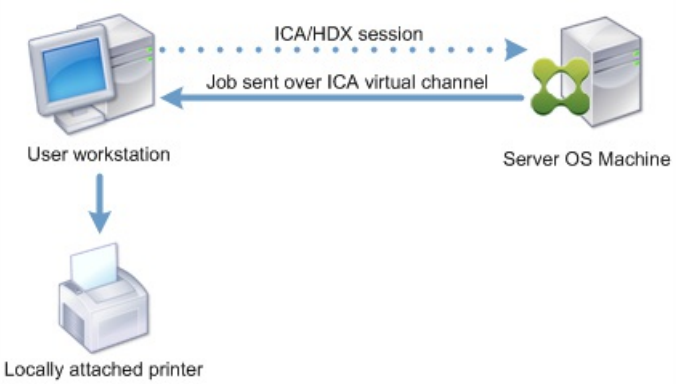
Print job routing

The term printing pathway encompasses both the path by which print jobs are routed and the location where print jobs are spooled. Both aspects of this concept are important. Routing affects network traffic. Spooling affects utilization of local resources on the device that processes the job.

In this environment, print jobs can take two paths to a printing device: through the client or through a network print server. Those paths are referred to as the client printing pathway and the network printing pathway. Which path is chosen by default depends on the kind of printer used.

Locally attached printers

The system routes jobs to locally attached printers from the Server OS machine, through the client, and then to the print device. The ICA protocol optimizes and compresses the print job traffic. When a printing device is attached locally to the user device, print jobs are routed over the ICA virtual channel.



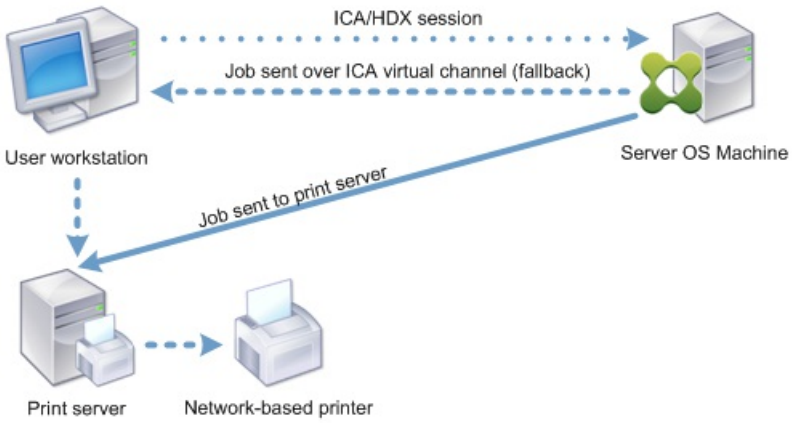
Network-based printers

By default, all print jobs destined for network printers route from the Server OS machine, across the network, and directly to the print server. However, print jobs are automatically routed over the ICA connection in the following situations:

- If the virtual desktop or application cannot contact the print server.
- If the native printer driver is not available on the Server OS machine.

If the Universal Print Server is not enabled, configuring the client printing pathway for network printing is useful for low bandwidth connections, such as wide area networks, that can benefit from the optimization and traffic compression that results from sending jobs over the ICA connection.

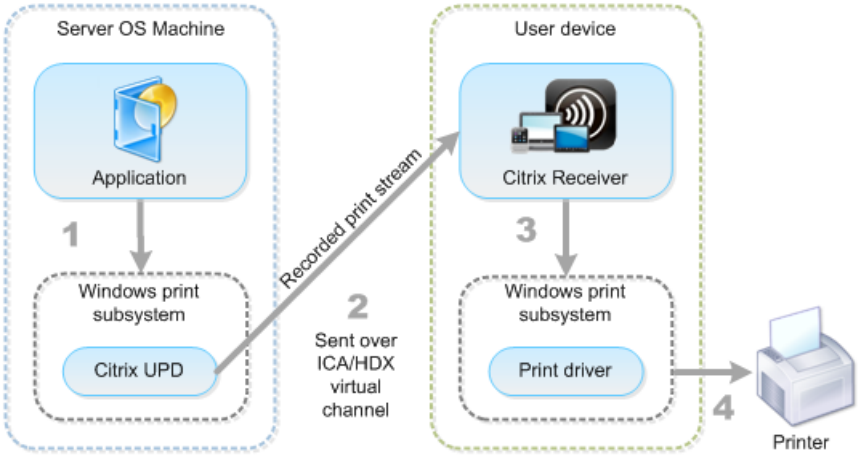
The client printing pathway also lets you limit traffic or restrict bandwidth allocated for print jobs. If routing jobs through the user device is not possible, such as for thin clients without printing capabilities, Quality of Service should be configured to prioritize ICA/HDX traffic and ensure a good in-session user experience.



Print driver management

To simplify printing in this environment, Citrix recommends using Citrix Universal print driver. The Universal print driver is a device-independent driver that supports any print device and thus simplifies administration by reducing the number of drivers required.

The following illustration shows the Universal print driver components and a typical workflow for a printer locally attached to a device.

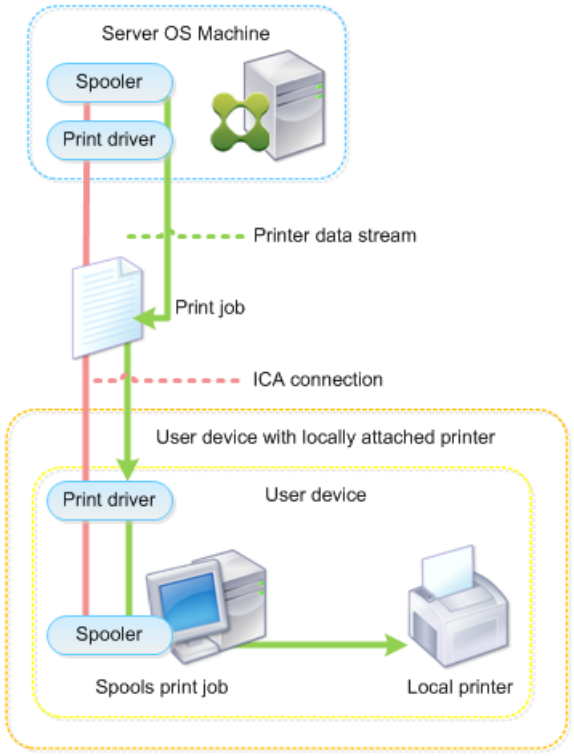


When planning your driver management strategy, determine if you will support the Universal print driver, device-specific drivers, or both. If you support standard drivers, you need to determine:

- The types of drivers to support.
- Whether to install printer drivers automatically when they are missing from Server OS machines.
- Whether to create driver compatibility lists.

During printer autocreation, if the system detects a new local printer connected to a user device, it checks the Server OS machine for the required printer driver. By default, if a Windows-native driver is not available, the system uses the Universal print driver.

The printer driver on the Server OS machine and the driver on the user device must match for printing to succeed. The illustration that follows shows how a printer driver is used in two places for client printing.



Related content

- Printing configuration example
- Best practices, security considerations, and default operations
- Print policies and preferences
- Provision printers
- Maintain the printing environment
- Universal Print Server Requirements

Printing configuration example

Sep 09, 2015

Choosing the most appropriate printing configuration options for your needs and environment can simplify administration. Although the default print configuration enables users to print in most environments, the defaults might not provide the expected user experience or the optimum network usage and management overhead for your environment.

Your printing configuration depends upon:

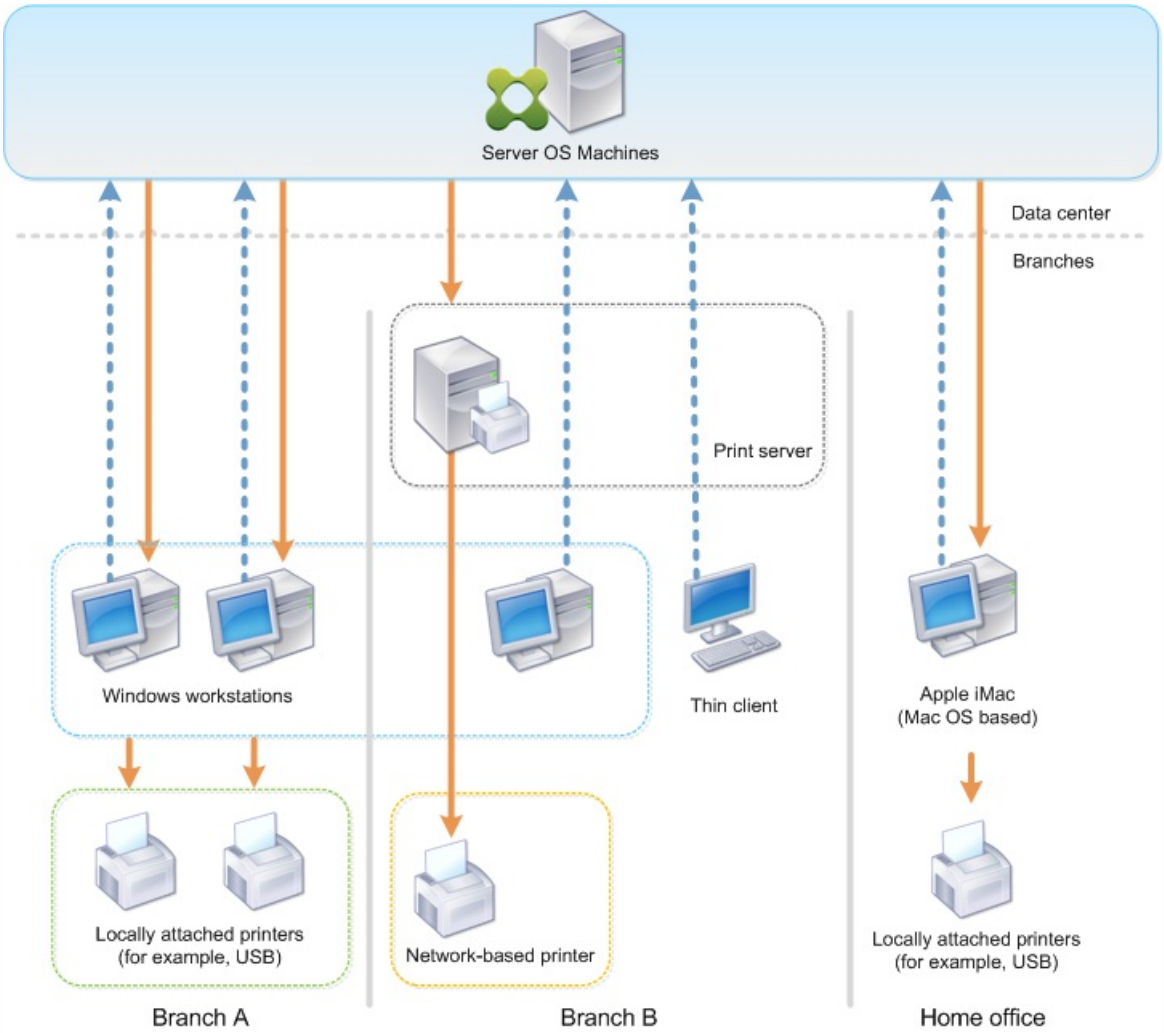
- Your business needs and your existing printing infrastructure.
  Design your printing configuration around the needs of your organization. Your existing printing implementation (whether users can add printers, which users have access to what printers, and so on) might be a useful guide when defining your printing configuration.
- Whether your organization has security policies that reserve printers for certain users (for example, printers for Human Resources or payroll).
- Whether users need to print while away from their primary work location, such as workers who move between workstations or travel on business.

When designing your printing configuration, try to give users the same experience in a session as they have when printing from local user devices.

Example print deployment

The following illustration shows the print deployment for these use cases:

- **Branch A –** A small overseas branch office with a few Windows workstations. Every user workstation has a locally attached, private printer.
- **Branch B –** A large branch office with thin clients and Windows-based workstations. For increased efficiency, the users of this branch share network-based printers (one per floor). Windows-based print servers located within the branch manage the print queues.
- **Home office –** A home office with a Mac OS-based user device that accesses the company's Citrix infrastructure. The user device has a locally attached printer.



The following sections describe the configurations which minimize the complexity of the environment and simplify its management.

Auto-created client printers and Citrix Universal printer driver

In Branch A, all users work on Windows-based workstations, therefore auto-created client printers and the Universal printer driver are used. Those technologies provide these benefits:

- Performance – Print jobs are delivered over the ICA printing channel, thus the print data can be compressed to save bandwidth.
  To ensure that a single user printing a large document cannot degrade the session performance of other users, a Citrix policy is configured to specify the maximum printing bandwidth.

  An alternative solution is to leverage a multi-stream ICA connection, in which the print traffic is transferred within a separate low priority TCP connection. Multi-stream ICA is an option when Quality of Service (QoS) is not implemented on the WAN connection.

- Flexibility – Use of the Citrix Universal printer driver ensures that all printers connected to a client can also be used from a virtual desktop or application session without integrating a new printer driver in the data center.

Citrix Universal Print Server

In Branch B, all printers are network-based and their queues are managed on a Windows print server, thus the Citrix Universal Print Server is the most efficient configuration.

All required printer drivers are installed and managed on the print server by local administrators. Mapping the printers into the virtual desktop or application session works as follows:

- For Windows-based workstations – The local IT team helps users connect the appropriate network-based printer to their Windows workstations. This enables users to print from locally-installed applications.
  During a virtual desktop or application session, the printers configured locally are enumerated through autocreation. The virtual desktop or application then connects to the print server as a direct network connection if possible.

  The Citrix Universal Print Server components are installed and enabled, thus native printer drivers are not required. If a driver is updated or a printer queue is modified, no additional configuration is required in the data center.

- For thin clients – For thin client users, printers must be connected within the virtual desktop or application session. To provide users with the simplest printing experience, administrators configure a single Citrix Session Printer policy per floor to connect a floor's printer as the default printer.
  To ensure the correct printer is connected even if users roam between floors, the policies are filtered based on the subnet or the name of the thin client. That configuration, referred to as proximity printing, allows for local printer driver maintenance (according to the delegated administration model).

  If a printer queue needs to be modified or added, Citrix administrators must modify the respective Session printer policy within the environment.

Because the network printing traffic will be sent outside the ICA virtual channel, QoS is implemented. Inbound and outbound network traffic on ports used by ICA/HDX traffic are prioritized over all other network traffic. That configuration ensures that user sessions are not impacted by large print jobs.

Auto-created client printers and Citrix Universal printer driver

For home offices where users work on non-standard workstations and use non-managed print devices, the simplest approach is to use auto-created client printers and the Universal printer driver.

Deployment summary

In summary, the sample deployment is configured as follows:

- No printer drivers are installed on Server OS machines. Only the Citrix Universal printer driver is used. Fallback to native printing and the automatic installation of printer drivers are disabled.
- A policy is configured to auto-create all client printers for all users. Server OS machines will directly connect to the print servers by default. The only configuration required is to enable the Universal Print Server components.
- A session printer policy is configured for every floor of Branch B and applied to all thin clients of the respective floor.
- QoS is implemented for Branch B to ensure excellent user experience.

Best practices, security considerations, and default operations

Oct 16, 2015

Best practices

Many factors determine the best printing solution for a particular environment. Some of these best practices might not apply to your Site.

- Use the Citrix Universal Print Server.
- Use the Universal printer driver or Windows-native drivers.
- Minimize the number of printer drivers installed on Server OS machines.
- Use driver mapping to native drivers.
- Never install untested printer drivers on a production site.
- Avoid updating a driver. Always attempt to uninstall a driver, restart the print server, and then install the replacement driver.
- Uninstall unused drivers or use the Printer driver mapping and compatibility policy to prevent printers from being created with the driver.
- Try to avoid using version 2 kernel-mode drivers.
- To determine if a printer model is supported, contact the manufacturer or see the Citrix Ready product guide at www.citrix.com/ready.
  In general, all of the Microsoft-supplied printer drivers are tested with Terminal Services and guaranteed to work with Citrix. However, before using a third-party printer driver, consult your printer driver vendor to ensure the driver is certified for Terminal Services by the Windows Hardware Quality Labs (WHQL) program. Citrix does not certify printer drivers.

Security considerations

Citrix printing solutions are secure by design.

- The Citrix Print Manager Service constantly monitors and responds to session events such as logon and logoff, disconnect, reconnect, and session termination. It handles service requests by impersonating the actual session user.
- Citrix printing assigns each printer a unique namespace in a session.
- Citrix printing sets the default security descriptor for auto-created printers to ensure that client printers auto-created in one session are inaccessible to users running in other sessions. By default, administrative users cannot accidentally print to another session's client printer, even though they can see and manually adjust permissions for any client printer.

Default print operations

By default, if you do not configure any policy rules, printing behavior is as follows:

- The Universal Print Server is disabled.
- All printers configured on the user device are created automatically at the beginning of each session.
  This behavior is equivalent to configuring the Citrix policy setting Auto-create client printers with the Auto-create all client printers option.
- The system routes all print jobs queued to printers locally attached to user devices as client print jobs (that is, over the ICA channel and through the user device).
- The system routes all print jobs queued to network printers directly from Server OS machines. If the system cannot route the jobs over the network, it will route them through the user device as a redirected client print job.
  This behavior is equivalent to disabling the Citrix policy setting Direct connection to print servers.

- The system attempts to store printing properties, a combination of the user's printing preferences and printing device-specific settings, on the user device. If the client does not support this operation, the system stores printing properties in user profiles on the Server OS machine.
  This behavior is equivalent to configuring the Citrix policy setting Printer properties retention with the Held in profile only if not saved on client option.

- The system uses the Windows version of the printer driver if it is available on the Server OS machine. If the printer driver is not available, the system attempts to install the driver from the Windows operating system. If the driver is not available in Windows, it uses a Citrix Universal print driver.
  This behavior is equivalent to enabling the Citrix policy setting Automatic installation of in-box printer drivers and configuring the Universal printing setting with the Use universal printing only if requested driver is unavailable.

  Enabling Automatic installation of in-box printer drivers might result in the installation of a large number of native printer drivers.

Note: If you are unsure about what the shipping defaults are for printing, display them by creating a new policy and setting all printing policy rules to Enabled. The option that appears is the default.

Always-On logging

XenApp and XenDesktop 7.6 FP3 includes an Always-On logging feature for the print server and printing subsystem on the VDA.

In order to collate the logs as a ZIP for emailing, or to automatically upload to Citrix Insights Services, use the PowerShell cmdlet (Start-TelemetryUpload) supplied with the VDA installer in 7.6 FP3.

Print policies and preferences

Sep 09, 2015

When users access printers from published applications, you can configure Citrix policies to specify:

- How printers are provisioned (or added to sessions)
- How print jobs are routed
- How printer drivers are managed

You can have different printing configurations for different user devices, users, or any other objects on which policies are filtered.

Most printing functions are configured through the Citrix Printing policies. Printing settings follow standard Citrix policy behavior.

The system can write printer settings to the printer object at the end of a session or to a client printing device, provided the user's network account has sufficient permissions. By default, Receiver uses the settings stored in the printer object in the session, before looking in other locations for settings and preferences.

By default, the system stores, or retains, printer properties on the user device (if supported by the device) or in the user profile on the Server OS machine. When a user changes printer properties during a session, those changes are updated in the user profile on the machine. The next time the user logs on or reconnects, the user device inherits those retained settings. That is, printer property changes on the user device do not impact the current session until after the user logs off and then logs on again.

Printing preference locations

In Windows printing environments, changes made to printing preferences can be stored on the local computer or in a document. In this environment, when users modify printing settings, the settings are stored in these locations:

- **On the user device itself –** Windows users can change device settings on the user device by right-clicking the printer in the Control Panel and selecting Printing Preferences. For example, if Landscape is selected as page orientation, landscape is saved as the default page orientation preference for that printer.
- **Inside of a document –** In word-processing and desktop-publishing programs, document settings, such as page orientation, are often stored inside documents. For example, when you queue a document to print, Microsoft Word typically stores the printing preferences you specified, such as page orientation and the printer name, inside the document. These settings appear by default the next time you print that document.
- **From changes a user made during a session –** The system keeps only changes to the printing settings of an auto-created printer if the change was made in the Control Panel in the session; that is, on the Server OS machine.
- **On the Server OS machine –** These are the default settings associated with a particular printer driver on the machine.

The settings preserved in any Windows-based environment vary according to where the user made the changes. This also means that the printing settings that appear in one place, such as in a spreadsheet program, can be different than those in others, such as documents. As result, printing settings applied to a specific printer can change throughout a session.

Hierarchy of user printing preferences

Because printing preferences can be stored in multiple places, the system processes them according to a specific priority. Also, it is important to note that device settings are treated distinctly from, and usually take precedence over, document settings.

By default, the system always applies any printing settings a user modified during a session (that is, the retained settings) before considering any other settings. When the user prints, the system merges and applies the default printer settings stored on the Server OS machine with any retained or client printer settings.

Saving user printing preferences

Citrix recommends that you do not change where the printer properties are stored. The default setting, which saves the printer properties on the user device, is the easiest way to ensure consistent printing properties. If the system is unable to save properties on the user device, it automatically falls back to the user profile on the Server OS machine.

Review the Printer properties retention policy setting if these scenarios apply:

- If you use legacy plug-ins that do not allow users to store printer properties on a user device.
- If you use mandatory profiles on your Windows network and want to retain the user's printer properties.

Provision printers

Mar 02, 2016

There are three printer provisioning methods:

- Citrix Universal Print Server
- Auto-created client printers
- Assign network printers to users

Citrix Universal Print Server

When determining the best print solution for your environment, consider the following:

- The Universal Print Server provides features not available for the Windows Print Provider: Image and font caching, advanced compression, optimization, and QoS support.
- The Universal print driver supports the public device-independent settings defined by Microsoft. If users need access to device settings that are specific to a print driver manufacturer, the Universal Print Server paired with a Windows-native driver might be the best solution. With that configuration, you retain the benefits of the Universal Print Server while providing users access to specialized printer functionality. A trade-off to consider is that Windows-native drivers require maintenance.
- The Citrix Universal Print Server provides universal printing support for network printers. The Universal Print Server uses the Universal print driver, a single driver on the Server OS machine that allows local or network printing from any device, including thin clients and tablets.

To use the Universal Print Server with a Windows-native driver, enable the Universal Print Server. By default, if the Windows-native driver is available, it is used. Otherwise, the Universal print driver is used. To specify changes to that behavior, such as to use only the Windows-native driver or only the Universal print driver, update the Universal print driver usage policy setting.

Install the Citrix Universal Print Server (UPS)

In XenApp and XenDesktop 7.6 FP3, the UPS package contains updated versions of the standalone UPS client and server components.

The UPServer component, which you install on print servers, is now supported on Windows Server 2012 R2 and Windows Server 2012.

Check the latest System Requirements for the UPServer component.

The UPClient component, that you install on XenApp and XenDesktop hosts which provision session network printers, is compatible with Windows 10 desktops and is part of the VDA installation.

User authentication during printing operations requires the Universal Print Server to be joined to the same domain as the Remote Desktop Services VDA.

To install the Citrix Universal Print Server:

1. Download the Universal Print Server installation package, UpsServer_7.6.300.zip.
2. Install the UPServer component by extracting and then launching the component's MSI, UpsServer_x64.msi or UpsServer_x86.msi.
3. A restart is required after installing the UPServer component.

For environments where you want to deploy the UPClient component separately, for example with **XenApp 6.5**:

1. Download the XenApp and XenDesktop 7.6 FP3 Virtual Delivery Agent (VDA) standalone package for Windows Desktop OS or Windows Server OS.
2. Extract the VDA using the command line instructions described in Install VDAs using the standalone package.
3. Install the pre-requisites from the \Image-Full\Support\VcRedist_2013_RTM
   - Vcredist_x64 / vcredist_x86
     - Run x86 for 32-bit only, and both for 64-bit deployments
4. Install the cdf pre-requisite from the \Image-Full\x64\Virtual Desktop Components or \Image-Full\x86\Virtual Desktop Components.
   - Cdf_x64 / Cdf_x86
     - x86 for 32-bit, x64 for 64-bit
5. Find the UPClient component in \Image-Full\x64\Virtual Desktop Components or \Image-Full\x86\Virtual Desktop Components.
6. Install the UPClient component by extracting and then launching the component's MSI.
7. A restart is required after installing the UPClient component.

Configure the Universal Print Server

Use the following Citrix policy settings to configure the Universal Print Server. For more information, refer to the on-screen policy settings help.

- **Universal Print Server enable**. Universal Print Server is disabled by default. When you enable Universal Print Server, you choose whether to use the Windows Print Provider if the Universal Print Server is unavailable. After you enable the Universal Print Server, a user can add and enumerate network printers through the Windows Print Provider and Citrix Provider interfaces.
- **Universal Print Server print data stream (CGP) port**. Specifies the TCP port number used by the Universal Print Server print data stream CGP (Common Gateway Protocol) listener. Defaults to **7229**.
- **Universal Print Server web service (HTTP/SOAP) port**. Specifies the TCP port number used by the Universal Print Server listener for incoming HTTP/SOAP requests. Defaults to **8080**.

  To change the default port of HTTP 8080 for Universal Print Server communication to XenApp and XenDesktop VDAs, the following registry must also be created and the port number value modified on the Universal Print Server computer(s):

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies
  "UpsHttpPort"=DWORD:<portnumber>

  This port number must match the HDX Policy, Universal Print Server web service (HTTP/SOAP) port, in Studio.

- **Universal Print Server print stream input bandwidth limit (kbps)**. Specifies the upper bound (in kilobits-per-second) for the transfer rate of print data delivered from each print job to the Universal Print Server using CGP. Defaults to 0 (unlimited).

Interactions with other policy settings

The Universal Print Server honors other Citrix printing policy settings and interacts with them as noted in the following table. The information provided assumes that the Universal Print Server policy setting is enabled, the Universal Print Server components are installed, and the policy settings are applied.

Policy setting	Interaction
Client printer	After the Universal Print Server is enabled, client network printers are created using the Universal

Policy setting	Interaction
redirection, Auto-create client printers	print driver instead of the native drivers. Users see the same printer name as before.
Session printers	When you use the Citrix Universal Print Server solution, Universal print driver policy settings are honored.
Direct connections to print server	When the Universal Print Server is enabled and the Universal print driver usage policy setting is configured to use universal printing only, a direct network printer can be created to the print server, using the Universal print driver.
UPD preference	Supports EMF and XPS drivers.

Effects on user interfaces

The Citrix Universal print driver used by the Universal Print Server disables the following user interface controls:

- In the Printer Properties dialog box, the Local Printer Settings button
- In the Document Properties dialog box, the Local Printer Settings and Preview on client buttons

When using the Universal Print Server, the Add Printer Wizard for the Citrix Print Provider is the same as the Add Printer Wizard for the Windows Print Provider, with the following exceptions:

- When adding a printer by name or address, you can provide an HTTP/SOAP port number for the print server. That port number becomes a part of the printer name and appears in displays.
- If the Citrix Universal print driver usage policy setting specifies that universal printing must be used, the Universal print driver name appears when selecting a printer. The Windows Print Provider cannot use the Universal print driver.

The Citrix Print Provider does not support client-side rendering.

For more information about the Universal Print Server, see CTX200328.

Auto-created client printers

These universal printing solutions are provided for client printers:

- **Citrix Universal Printer -** A generic printer created at the beginning of sessions that is not tied to a printing device. The Citrix Universal Printer is not required to enumerate the available client printers during logon, which can greatly reduce resource usage and decrease user logon times. The Universal Printer can print to any client-side printing device.
  The Citrix Universal Printer might not work for all user devices or Receivers in your environment. The Citrix Universal Printer requires a Windows environment and does not support the Citrix Offline Plug-in or applications that are streamed to the client. Consider using auto-created client printers and the Universal print driver for such environments.

  To use a universal printing solution for non-Windows Receivers, use one of the other Universal print drivers that are based on postscript/PCL and installed automatically.

- **Citrix Universal print drivers -** A device-independent printer driver. If you configure a Citrix Universal print driver, the system uses the EMF-based Universal print driver by default.
  The Citrix Universal print driver might create smaller print jobs than older or less advanced printer drivers. However, a device-specific driver might be needed to optimize print jobs for a specialized printer.

Configure universal printing - Use the following Citrix policy settings to configure universal printing. For more information, refer to the on-screen policy settings help.

- Universal print driver usage. Specifies when to use universal printing.

- Auto-create generic universal printer. Enables or disables auto-creation of the generic Citrix Universal Printer object for sessions when a user device compatible with Universal Printing is in use. By default, the generic Universal Printer object is not auto-created.
- Universal driver preference. Specifies the order in which the system attempts to use Universal print drivers, beginning with the first entry in the list. You can add, edit, or remove drivers and change the order of the drivers in the list.
- Universal printing preview preference. Specifies whether to use the print preview function for auto-created or generic universal printers.
- Universal printing EMF processing mode. Controls the method of processing the EMF spool file on the Windows user device. By default, EMF records are spooled directly to the printer. Spooling directly to the printer allows the spooler to process the records faster and uses fewer CPU resources.

For more policies, see Optimize printing performance. To change the defaults for settings such as paper size, print quality, color, duplex, and the number of copies, see CTX113148.

Auto-create printers from the user device - At the start of a session, the system auto-creates all printers on the user device by default. You can control what, if any, types of printers are provisioned to users and prevent autocreation.

Use the Citrix policy setting Auto-create client printers to control autocreation. You can specify that:
- All printers visible to the user device, including network and locally attached printers, are created automatically at the start of each session (default)
- All local printers physically attached to the user device is created automatically
- Only the default printer for the user device is created automatically
- Autocreation is disabled for all client printers

The Auto-create client printers setting requires that the Client printer redirection setting is Allowed (the default).

Assign network printers to users

By default, network printers on the user device are created automatically at the beginning of sessions. the system enables you to reduce the number of network printers that are enumerated and mapped by specifying the network printers to be created within each session. Such printers are referred to as session printers.

You can filter session printer policies by IP address to provide proximity printing. Proximity printing enables users within a specified IP address range to automatically access the network printing devices that exist within that same range. Proximity printing is provided by the Citrix Universal Print Server and does not require the configuration described in this section.

Proximity printing might involve the following scenario:
- The internal company network operates with a DHCP server which automatically designates IP addresses to users.
- All departments within the company have unique designated IP address ranges.
- Network printers exist within each department's IP address range.

When proximity printing is configured and an employee travels from one department to another, no additional printing device configuration is required. Once the user device is recognized within the new department's IP address range, it will have access to all network printers within that range.

Configure specific printers to be redirected in sessions - To create administrator-assigned printers, configure the Citrix policy setting Session printers. Add a network printer to that policy using one of the following methods:
- Enter the printer UNC path using the format \\servername\printername.
- Browse to a printer location on the network.
- Browse for printers on a specific server. Enter the server name using the format \\servername and click Browse.

Important: The server merges all enabled session printer settings for all applied policies, starting from the highest to lowest priorities. When a printer is configured in multiple policy objects, custom default settings are taken from only the highest priority policy object in which that printer is configured.
Network printers created with the Session printers setting can vary according to where the session was initiated by filtering on objects such as subnets.

Specify a default network printer for a session - By default, the user's main printer is used as the default printer for the session. Use the Citrix policy setting Default printer to change how the default printer on the user device is established in a session.

1. On the Default printer settings page, select a setting for Choose client's default printer:
   - Network printer name. Printers added with the Session printers policy setting appear in this menu. Select the network printer to use as the default for this policy.
   - Do not adjust the user's default printer. Uses the current Terminal Services or Windows user profile setting for the default printer. For more information, refer to the on-screen policy settings help.
2. Apply the policy to the group of users (or other filtered objects) you want to affect.

Configure proximity printing - Proximity printing is also provided by the Citrix Universal Print Server, which does not require the configuration described here.

1. Create a separate policy for each subnet (or to correspond with printer location).
2. In each policy, add the printers in that subnet's geographic location to the Session printers setting.
3. Set the Default printer setting to Do not adjust the user's default printer.
4. Filter the policies by client IP address. Be sure to update these policies to reflect changes to the DHCP IP address ranges.

Maintain the printing environment

Sep 09, 2015

Maintaining the printing environment includes:

- Managing printer drivers
- Optimizing printing performance
- Displaying printer and managing print queues

Manage printer drivers

To minimize administrative overhead and the potential for print driver issues, Citrix recommends use of the Citrix Universal print driver.

If auto-creation fails, by default, the system installs a Windows-native printer driver provided with Windows. If a driver is not available, the system falls back to the Universal print driver. For more information about printer driver defaults, refer to Best practices, security considerations, and default operations.

If the Citrix Universal print driver is not an option for all scenarios, map printer drivers to minimize the amount of drivers installed on Server OS machines. In addition, mapping printer drivers enables you to:

- Allow specified printers to use only the Citrix Universal print driver
- Allow or prevent printers to be created with a specified driver
- Substitute good printer drivers for outdated or corrupted drivers
- Substitute a driver that is available on Windows server for a client driver name

Prevent the automatic installation of printer drivers - The automatic installation of print drivers should be disabled to ensure consistency across Server OS machines. This can be achieved through Citrix policies, Microsoft policies, or both. To prevent the automatic installation of Windows-native printer drivers, disable the Citrix policy setting Automatic installation of in-box printer drivers.

Map client printer drivers - Each client provides information about client-side printers during logon, including the printer driver name. During client printer autocreation, Windows server printer driver names are selected that correspond to the printer model names provided by the client. The autocreation process then uses the identified, available printer drivers to construct redirected client print queues.

Here is the general process for defining driver substitution rules and editing print settings for mapped client printer drivers:

1. To specify driver substitution rules for auto-created client printers, configure the Citrix policy setting Printer driver mapping and compatibility by adding the client printer driver name and selecting the server driver that you want to substitute for the client printer driver from the Find printer driver menu. You can use wildcards in this setting. For example, to force all HP printers to use a specific driver, specify HP* in the policy setting.
2. To ban a printer driver, select the driver name and choose the Do not create setting.
3. As needed, edit an existing mapping, remove a mapping, or change the order of driver entries in the list.
4. To edit the printing settings for mapped client printer drivers, select the printer driver, click Settings, and specify settings such as print quality, orientation, and color. If you specify a printing option that the printer driver does not support, that option has no effect. This setting overrides retained printer settings the user set during a previous session.
5. Citrix recommends testing the behavior of the printers in detail after mapping drivers, since some printer functionality can be available only with a specific driver.

When users log on the system checks the client printer driver compatibility list before it sets up the client printers.

Optimize printing performance

To optimize printing performance, use the Universal Print Server and Universal print driver. The following policies control printing optimization and compression:

- Universal printing optimization defaults. Specifies default settings for the Universal Printer when it is created for a session:
  - Desired image quality specifies the default image compression limit applied to universal printing. By default, Standard Quality is enabled, meaning that users can only print images using standard or reduced quality compression.
  - Enable heavyweight compression enables or disables reducing bandwidth beyond the compression level set by Desired image quality, without losing image quality. By default, heavyweight compression is disabled.
  - Image and Font Caching settings specify whether or not to cache images and fonts that appear multiple times in the print stream, ensuring each unique image or font is sent to the printer only once. By default, embedded images and fonts are cached.
  - Allow non-administrators to modify these settings specifies whether or not users can change the default print optimization settings within a session. By default, users are not allowed to change the default print optimization settings.
- Universal printing image compression limit. Defines the maximum quality and the minimum compression level available for images printed with the Universal print driver. By default, the image compression limit is set to Best Quality (lossless compression).
- Universal printing print quality limit. Specifies the maximum dots per inch (dpi) available for generating printed output in the session. By default, no limit is specified.

By default, all print jobs destined for network printers route from the Server OS machine, across the network, and directly to the print server. Consider routing print jobs over the ICA connection if the network has substantial latency or limited bandwidth. To do that, disable the Citrix policy setting Direct connections to print servers. Data sent over the ICA connection is compressed, so less bandwidth is consumed as the data travels across the WAN.

Improve session performance by limiting printing bandwidth - While printing files from Server OS machines to user printers, other virtual channels (such as video) may experience decreased performance due to competition for bandwidth especially if users access servers through slower networks. To prevent such degradation, you can limit the bandwidth used by user printing. By limiting the data transmission rate for printing, you make more bandwidth available in the HDX data stream for transmission of video, keystrokes, and mouse data.

Important: The printer bandwidth limit is always enforced, even when no other channels are in use.
Use the following Citrix policy Bandwidth printer settings to configure printing bandwidth session limits. To set the limits for the site, perform this task using Studio. To set the limits for individual servers, perform this task using the Group Policy Management Console in Windows locally on each Server OS machine.

- The Printer redirection bandwidth limit setting specifies the bandwidth available for printing in kilobits per second (kbps).
- The Printer redirection bandwidth limit percent setting limits the bandwidth available for printing to a percentage of the overall bandwidth available.
  Note: To specify bandwidth as a percentage using the Printer redirection bandwidth limit percent setting, enable the Overall session bandwidth limit as well.
  If you enter values for both settings, the most restrictive setting (the lower value) is applied.

To obtain real-time information about printing bandwidth, use Citrix Director.

Display printers and manage print queues

The following table summarizes where you can display printers and manage print queues in your environment.

	Printing Pathway	UAC Enabled?	Location
Client printers (Printers attached to the user device)	Client printing pathway	On	Print Management snap-in located in the Microsoft Management Console
		Off	Pre-Windows 8: Control Panel Windows 8: Print Management snap-in
Network printers (Printers on a network print server)	Network printing pathway	On	Print Server > Print Management snap-in located in the Microsoft Management Console
		Off	Print Server > Control Panel
Network printers (Printers on a network print server)	Client printing pathway	On	Print Server > Print Management snap-in located in the Microsoft Management Console
		Off	Pre-Windows 8: Control Panel Windows 8: Print Management snap-in
Local network server printers (Printers from a network print server that are added to a Server OS machine)	Network printing pathway	On	Print Server > Control Panel
		Off	Print Server > Control Panel

Note: Print queues for network printers that use the network printing pathway are private and cannot be managed through the system.

Licensing

Sep 09, 2015

From Studio, you can manage and track licensing, if the license server is in the same domain as Studio or in a trusted domain. For information about other licensing tasks, see

— Licensing Your Product

.

You must be a full license administrator to complete the tasks described below, except for viewing license information. To view license information in Studio, an administrator must have at least the Read Licensing Delegated Administration permission; the built-in Full Administrator and Read-Only Administrator roles have that permission.

The following table lists the supported editions and license models:

Products	Editions	License models
XenApp	• Platinum • Enterprise • Advanced	Concurrent
XenDesktop	• Platinum • Enterprise • App • VDI	• User/Device • Concurrent

To view license information, in the Studio navigation pane, select Configuration and then Licensing. A summary of license usage and settings for the site is displayed with a list of all the licenses currently installed on the specified license server.

To manage licensing, in the Studio navigation pane, select Configuration and then Licensing. Then:

- To download a license from Citrix:
  1. In the Actions pane, select Allocate Licenses.
  2. Type the License Access Code, which is supplied in an email from Citrix.
  3. Select a product and click Allocate Licenses. All the licenses available for that product are allocated and downloaded. After you allocate and download all the licenses for a specific License Access Code, you cannot use that License Access Code again. To perform additional transactions with that code, log on to My Account.
- To add licenses that are stored on your local computer or on the network:
  1. In the Actions pane, select Add Licenses.
  2. Browse to a license file and add it to the license server.
- To change the license server:
  1. In the Actions pane, select Change License Server.
  2. Type the address of the license server in the form name:port, where name is a DNS, NetBIOS, or IP address. If you do not specify a port number, the default port (27000) is used.
- To select the type of license to use:
  - When configuring the Site, after you specify the license server, you are prompted to select the type of license to use. If there are no licenses on the server, the option to use the product for a 30-day trial period without a license is automatically selected.

    - If there are licenses on the server, their details are displayed and you can select one of them. Or, you can add a license file to the server and then select that one.
- To change the product edition and licensing model:
    1. In the Actions pane, select Edit Product Edition.
    2. Update the appropriate options.
- To access the License Administration Console, in the Actions pane, select License Administration Console. The console either appears immediately, or if the dashboard is configured as password-protected, you are prompted for License Administration Console credentials. For details about how to use the console, see *— Licensing Your Product* .
- To add a licensing administrator:
    1. In the middle pane, choose the Licensing Administrators tab.
    2. In the Actions pane, select Add licensing administrator.
    3. Browse to the user you want to add as an administrator and choose permissions.
- To edit or delete a licensing administrator, When you select an administrator, the options to Edit licensing administrator (to change the administrator permissions for that administrator) and Delete licensing administrator appear in the Actions pane.
    1. In the middle pane, choose the Licensing Administrators tab and select the administrator you want to delete or edit.
    2. In the Actions pane, select either Edit licensing administrator or Delete licensing administrator.
- To add a licensing administrator group:
    1. In the middle pane, choose the Licensing Administrators tab.
    2. In the Actions pane, select Add licensing administrator group.
    3. Browse to the group you want to act as licensing administrators and choose permissions. Adding an Active Directory Group gives licensing administrator permissions to the users within that group.
- To edit or delete a licensing administrator group:
    1. In the middle pane, choose the Licensing Administrators tab and select the administrator group you want to delete or edit. When you select a licensing administrator group, the options to Edit licensing administrator group (to change the administrator permissions for that group) and Delete licensing administrator group appear in the Actions pane..
    2. In the Actions pane, select either Edit licensing administrator group or Delete licensing administrator group.

Connections and resources

Sep 09, 2015

You create your first connection to hosting resources when you create a Site. Later, you can change that connection and create new ones. Read Only Administrators can view connection and resource details; you must be a Full Administrator to perform connection and resource management tasks.

Create a connection and resources

The hosting resources must be available before you create a connection.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select Add Connections and Resources in the Actions pane.
3. Select Create a new Connection.
4. On the Connection page:
   - Select the connection type and enter a connection name - choose a name that will help administrators identify the host type and deployment address. Additional required information depends on the selected connection type.

Connection type	Information needed
Citrix XenServer, Microsoft System Center Virtual Machine Manager, VMware vSphere, or Microsoft Configuration Manager Wake On LAN	Enter the connection URL, user name, and password. • For XenServer, Citrix recommends using HTTPS to secure communications. To use HTTPS, you must replace the default SSL certificate installed with XenServer with one from a trusted certificate authority; see CTX128656. • For XenServer, you can edit the new connection and select the high availability hypervisors to be used, if high availability is enabled on XenServer.
Citrix CloudPlatform or Amazon Web Services (AWS)	Enter the connection URL, API key and Secret key. • You can browse to an import keys file provided by your cloud administrator to fill in the API key and Secret key. • The credentials file for the root AWS account (retrieved from the AWS console) is not formatted the same as credentials files downloaded for standard AWS users. Therefore, Studio cannot use the file to populate the API key and Secret key fields. Ensure that you are using AWS IAM credentials files when using Studio in an AWS environment.

   - Choose the tools you will use to create virtual machines. For hypervisors that provide GPU resources, choose Studio Tools.
5. On the Storage page, select storage types and devices. When using Machine Creation Services, select the network and storage resources for the new virtual machines. If you use shared storage on XenServer connections, you can enable IntelliCache to reduce load on the storage device. For information about using IntelliCache, see below.
6. If the Connection has GPU capabilities, select the option to use graphics virtualization and then select a GPU type and group.
7. Enter a name for the resources.

Create a connection and resources from an existing connection

1. Select Configuration > Hosting in the Studio navigation pane.

2. Select Add Connection and Resources in the Actions pane.
3. Select Use an existing Connection and then choose the relevant connection.
4. Choose the tools you will use to create virtual machines. For hypervisors that provide GPU resources, choose Studio Tools. If the Connection has GPU capabilities, select the option to use graphics virtualization and then select a GPU type and group.
5. Enter a name for the resources.

Add storage

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select a connection and then select Add Storage in the Actions pane.
3. Select the storage to add.

Edit storage

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select a resources entry under a connection and then select Edit Storage in the Actions pane.
3. On the Standard Storage page, select or clear the check boxes for the storage locations that will store virtual machines.
   If you clear a storage location that was accepting new machines, it will no longer accept new machines. Existing machines will continue using that location (and write data to it); so it is possible for a storage location to become full even after it stops accepting new machines.
   If PvD storage is used, select or clear the check boxes on the PvD Storage page, too.

Edit a connection

Do not use this procedure to rename a connection or to create a new connection. Those are different operations.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Edit Connection in the Actions pane.
   - To change the connection address and credentials, on the Connection Properties page, click Edit settings and then enter the new information.
     You cannot change the GPU settings for a connection, because machine catalogs accessing this resource must use an appropriate GPU-specific master image. Create a new connection.
   - To specify the high-availability servers for a XenServer connection, on the Connection Properties page, click Edit HA servers. Citrix recommends that you select all servers in the pool to allow communication with XenServer if the pool master fails.
   - For a Microsoft System Center Configuration Manager (ConfMgr) Wake on LAN connection, on the Advanced page, enter ConfMgr Wake Proxy, magic packets, and packet transmission information.
   - To configure throttling based on thresholds of simultaneous actions on the connection, which can help when power management settings allow too many or too few machines to start at the same time.
     - On the Advanced page, for Simultaneous actions (all types) and Simultaneous Personal Storage inventory updates, specify two values: the maximum absolute number that can occur simultaneously on this connection, and a percentage of all machines using this connection. You must specify both absolute and percentage values, but the actual limit applied is the lower of the configured values.
       For example, in a deployment with 34 machines, if Simultaneous actions (all types) is set to an absolute value of 10 and a percentage value of 10, the actual limit applied is 3 (that is, 10 percent of 34 rounded to the nearest whole number, which is less than the absolute value of 10 machines).
     - Specify the maximum number of new actions per minute. This is an absolute number.

Note: Enter information in the Connection options field on the Advanced page only under the guidance of a Citrix Support representative.

Turn maintenance mode on or off for a connection

Turning on maintenance mode for a connection prevents any new power action from affecting any machine stored on the connection. Users cannot connect to a machine when it is in maintenance mode. If users are already connected, maintenance mode takes effect when they log off.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection. To turn maintenance mode on, select Turn On Maintenance Mode in the Actions pane. To turn maintenance mode off, select Turn Off Maintenance Mode.

You can also turn maintenance mode on or off for individual machines; see below.

Delete a connection

Caution: Deleting a connection can result in the deletion of large numbers of machines and loss of data. Ensure that user data on affected machines is backed up or no longer required.
Before you delete a Connection, ensure that:

- All users are logged off from the machines stored on the connection.
- No disconnected user sessions are running.
- Maintenance mode is turned on for pooled and dedicated machines.
- All machines in machine catalogs are powered off.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Delete Connection in the Actions pane.
3. If this connection has machines stored on it, you are asked whether the machines should be deleted. If they are to be deleted, specify what should be done with the associated Active Directory computer accounts.
   A machine catalog becomes unusable when you delete a connection that is referenced by that catalog. If this connection is referenced by a catalog, you have the option to delete the catalog. Before you delete a catalog, make sure it is not used by other connections.

Rename a connection

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Rename Connection in the Actions pane.

View machine details on a connection

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select View Machines in the Actions pane.

The upper pane lists the machines accessed through the connection. Select a machine to view its details in the lower pane. Session details are also provided for open sessions.

Use the search feature to find machines quickly. Either select a saved search from the list at the top of the window, or create a new search. You can either search by typing all or part of the machine name, or you can build an expression to use for an advanced search. To build an expression, click Unfold, and then select from the lists of properties and operators.

Manage machines on a connection

1. Select Configuration > Hosting in the Studio navigation pane.

2. Select a connection and then select View Machines in the Action pane.
3. Select one of the following in the Actions pane. Some actions may not be available, depending on the machine state and the connection host type.
   - Start - Starts the machine if it is powered off or suspended.
   - Suspend - Pauses the machine without shutting it down, and refreshes the list of machines.
   - Shut down - Requests the operating system to shut down.
   - Force shut down - Forcibly powers off the machine, and refreshes the list of machines.
   - Restart - requests the operating system to shut down and then start the machine again. If the operating system cannot comply, the desktop remains in its current state.
   - Enable maintenance mode - To temporarily stop connections to a machine, put it into maintenance mode. Users cannot connect to a machine in this state. If users are connected, maintenance mode takes effect when they log off.
     To turn maintenance mode on or off for all machines accessed through a connection, see above.
   - Remove from Delivery Group - Removing a machine from a Delivery Group does not delete it from the machine catalog that the Delivery Group uses. You can remove a machine only when no user is connected to it (turn on maintenance mode to temporarily prevent users from connecting while you are removing the machine).
   - Delete - When you delete a machine, users no longer have access to it, and the machine is deleted from the machine catalog. Before deleting a machine, ensure that all user data is backed up or no longer required. You can delete a machine only when no user is connected to it (turn on maintenance mode to temporarily stop users from connecting while you are deleting the machine).

   For actions that involve machine shutdown, if the machine does not shut down within 10 minutes, it is powered off. If Windows attempts to install updates during shutdown, there is a risk that the machine will be powered off before the updates are complete.

Delete, rename, or test resources

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the resource and then select the appropriate entry in the Actions pane: Delete Resources, Rename Resources, or Test Resources.

Use IntelliCache for XenServer connections

Using IntelliCache, hosted VDI deployments are more cost-effective because you can use a combination of shared storage and local storage. This enhances performance and reduces network traffic . The local storage caches the master image from the shared storage, which reduces the amount of reads on the shared storage. For shared desktops, writes to the differencing disks are written to local storage on the host and not to shared storage.

- Shared storage must be NFS when using IntelliCache.
- Citrix recommends that you use a high performance local storage device to ensure the fastest possible data transfer.

To use IntelliCache, you must enable it in both this product and XenServer.

- When installing XenServer, select Enable thin provisioning (Optimized storage for XenDesktop). Citrix does not support mixed pools of servers that have IntelliCache enabled and servers that do not. For more information, see the XenServer documentation.
- In XenApp and XenDesktop, IntelliCache is disabled by default. You can change the setting only when creating a XenServer connection; you cannot disable IntelliCache later. When you add a XenServer connection from Studio:
  - Select Shared as the storage type.
  - Select the Use IntelliCache check box.

Connection timers

You can use policy settings to configure three connection timers:

- A maximum connection timer. This setting determines the maximum duration of an uninterrupted connection between a user device and a virtual desktop. Use the Session connection timer and Session connection timer interval policy settings.
- A connection idle timer. This setting determines how long an uninterrupted user device connection to a virtual desktop will be maintained if there is no input from the user. Use the Session idle timer and Session idle timer interval policy settings.
- A disconnect timer. This setting determines how long a disconnected, locked virtual desktop can remain locked before the session is logged off. Use the Disconnected session timer and Disconnected session timer interval policy settings .

When you update any of these settings, ensure they are consistent across your deployment.

Connection leasing

Oct 27, 2015

To ensure that the Site database is always available, Citrix recommends starting with a fault-tolerant SQL Server deployment by following high availability best practices from Microsoft. However, network issues and interruptions may prevent Delivery Controllers from accessing the database, resulting in users not being able to connect to their applications or desktop.

The connection leasing feature supplements the SQL Server high availability best practices by enabling users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available.

Although users may have a large number of published resources available, they often use only a few of them regularly. When you enable connection leasing, each Controller caches user connections to those recently used applications and desktops during normal operations (when the database is available).

The leases generated on each Controller are uploaded to the Site database for periodic synchronization to other Controllers on the Site. In addition to leases, each Controller's cache holds application, desktop, icon, and worker information. The lease and related information is stored on each Controller's local disk. If the database becomes unavailable, the Controller enters leased connection mode and "replays" the cached operations when a user attempts to connect or reconnect to a recently used application or desktop from StoreFront.

Connections are cached for a lease period of two weeks. So, if the database becomes unavailable, the desktops and applications that the user launched in the previous two weeks remain accessible to that user through StoreFront. However, desktops and applications that have not been launched during the previous two-week lease period are not accessible when the database is unavailable. For example, if a user last launched an application three weeks ago, its lease has expired, and that user cannot launch that application if the database becomes unavailable now. Leases for long-running active or disconnected application or desktop sessions are extended so that they are not considered expired.

By default, connection leasing affects the entire Site; however, you can revoke all leases for specific users, which prevents them from accessing any applications or desktops when the Controller is in leased connection mode. Several other registry settings apply on a Controller basis.

Considerations and limitations

While connection leasing can improve connection resiliency and user productivity, there are considerations related to the availability, operation, and performance of other features.

Connection leasing is supported for server-hosted applications and desktops, and static (assigned) desktops; it is not supported for pooled VDI desktops or for users who have not been assigned a desktop when the database becomes unavailable.

When the Controller is in leased connection mode:

- Administrators cannot use Studio, Director, or the PowerShell console.
- Workspace Control is not available. When a user logs on to Receiver, sessions do not automatically reconnect; the user must relaunch the application.
- If a new lease is created immediately before the database becomes unavailable, but the lease information has not yet been synchronized across all Controllers, the user might not be able to launch that resource after the database becomes unavailable.
- Server-hosted application and desktop users may use more sessions than their configured session limits. For example:

    - A session may not roam when a user launches it from one device (connecting externally through NetScaler Gateway) when the Controller is not in leased connection mode and then connects from another device on the LAN when the Controller is in leased connection mode.
    - Session reconnection may fail if an application launches just before the database becomes unavailable; in such cases, a new session and application instance are launched.
- Static (assigned) desktops are not power-managed. VDAs that are powered off when the Controller enters leased connection mode remain unavailable until the database connection is restored, unless the administrator manually powers them on.
- If session prelaunch and session linger are enabled, new prelaunch sessions are not started. Prelaunched and lingering sessions will not be ended according to configured thresholds while the database is unavailable.
- Load management within the Site may be affected. Server-based connections are routed to the most recently used VDA. Load evaluators (and especially, session count rules) may be exceeded.
- The Controller will not enter leased connection mode if you use SQL Server Management Studio to take the database offline. Instead, use one of the following Transact-SQL statements:
    - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK IMMEDIATE
    - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK AFTER <seconds>

  Either statement cancels any pending transactions and causes the Controller to lose its connection with the database. The Controller then enters leased connection mode.

When connection leasing is enabled, there are two brief intervals during which users cannot connect or reconnect: (1) from the time the database becomes unavailable to when the Controller enters leased connection mode, and (2) from the time the Controller changes from leased connection mode to when database access is fully restored and the VDAs have re-registered.

For more considerations, see XenDesktop 7.6 Connection Leasing Design Considerations.

Configure and deploy

When configuring your deployment to accommodate connection leasing:

- VDAs must be at minimum version 7.6, and the machine catalogs and Delivery Groups that use those machines must be at that minimum level (or a later supported version).
- The Site database size requirements will increase.
- Each Controller needs additional disk space for the cached lease files.

Connection leasing is enabled by default.

You can turn connection leasing off or on from the PowerShell SDK or the Windows registry. From the PowerShell SDK, you can also remove current leases. The following PowerShell cmdlets affect connection leasing; see the cmdlet help for details.

- Set-BrokerSite -ConnectionLeasingEnabled $true|$false - Turns connection leasing on or off. Default = $true
- Get-BrokerServiceAddedCapability - Outputs “ConnectionLeasing” for the local Controller.
- Get-BrokerLease - Retrieves either all or a filtered set of current leases.
- Remove-BrokerLease - Marks either one or a filtered set of leases for deletion.
- Update-BrokerLocalLeaseCache – Updates the connection leasing cache on the local Controller. The data is resynchronized during the next synchronization.

Virtual IP and virtual loopback

Sep 29, 2015

Note: These features are valid only for Windows Server 2008 R2 and Windows Server 2012 R2 machines. They do not apply to Windows Desktop OS machines.

The Microsoft virtual IP address feature provides a published application with a unique dynamically-assigned IP address for each session. The Citrix virtual loopback feature allows you to configure applications that depend on communications with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.*).

Certain applications, such as CRM and Computer Telephony Integration (CTI), use an IP address for addressing, licensing, identification, or other purposes and thus require a unique IP address or a loopback address in sessions. Other applications may bind to a static port, so attempts to launch additional instances of an application in a multiuser environment will fail because the port is already in use. For such applications to function correctly in a XenApp environment, a unique IP address is required for each device.

Virtual IP and virtual loopback are independent features. You can use either or both.

Administrator action synopsis:

- To use Microsoft virtual IP, enable and configure it on the Windows server.
- To use Citrix virtual loopback, configure two settings in a Citrix policy.

Virtual IP

When virtual IP is enabled and configured on the Windows server, each configured application running in a session appears to have a unique address. Users access these applications on a XenApp server in the same way they access any other published application. A process requires virtual IP in either of the following cases:

- The process uses a hard-coded TCP port number
- The process uses Windows sockets and requires a unique IP address or a specified TCP port number

To determine if an application needs to use virtual IP addresses:

1. Obtain the TCPView tool from Microsoft. This tool lists all applications that bind specific IP addresses and ports.
2. Disable the Resolve IP Addresses feature so that you see the addresses instead of host names.
3. Launch the application and use TCPView to see which IP addresses and ports are opened by the application and which process names are opening these ports.
4. Configure any processes that open the IP address of the server, 0.0.0.0, or 127.0.0.1.
5. To ensure that an application does not open the same IP address on a different port, launch an additional instance of the application.

How Microsoft Remote Desktop (RD) IP virtualization works

- Virtual IP addressing must be enabled on the Microsoft server.
  For example, in a Windows Server 2008 R2 environment, from Server Manager, expand Remote Desktop Services > RD Session Host Connections to enable the RD IP Virtualization feature and configure the settings to dynamically assign IP addresses using the Dynamic Host Configuration Protocol (DHCP) server on a per-session or per-program basis. See the Microsoft documentation for instructions.

- After the feature is enabled, at session start-up, the server requests dynamically-assigned IP addresses from the DHCP server.
- The RD IP Virtualization feature assigns IP addresses to remote desktop connections per-session or per-program. If you

assign IP addresses for multiple programs, they share a per-session IP address.
- After an address is assigned to a session, the session uses the virtual address rather than the primary IP address for the system whenever the following calls are made: bind¸closesocket¸connect, WSAConnect, WSAAccept, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyaddr, getnameinfo, getaddrinfo

When using the Microsoft IP virtualization feature within the Remote Desktop session hosting configuration, applications are bound to specific IP addresses by inserting a "filter" component between the application and Winsock function calls. The application then sees only the IP address it should use. Any attempt by the application to listen for TCP or UDP communications is bound to its allocated virtual IP address (or loopback address) automatically, and any originating connections opened by the application originate from the IP address bound to the application.

In functions that return an address (such as GetAddrInfo(), which is controlled by a Windows policy), if the local host IP address is requested, virtual IP looks at the returned IP address and changes it to the virtual IP address of the session. Applications that attempt to get the IP address of the local server through such name functions see only the unique virtual IP address assigned to that session. This IP address is often used in subsequent socket calls, such as bind or connect.

Often, an application requests to bind to a port for listening on the address 0.0.0.0. When an application does this and uses a static port, you cannot launch more than one instance of the application. The virtual IP address feature also looks for 0.0.0.0 in these call types and changes the call to listen on the specific virtual IP address, which enables more than one application to listen on the same port on the same computer because they are all listening on different addresses. The call is changed only if it is in an ICA session and the virtual IP address feature is enabled. For example, if two instances of an application running in different sessions both try to bind to all interfaces (0.0.0.0) and a specific port (such as 9000), they are bound to VIPAddress1:9000 and VIPAddress2:9000 and there is no conflict.

Virtual loopback

Enabling the Citrix virtual IP loopback policy settings allows each session to have its own loopback address for communication. When an application uses the localhost address (default = 127.0.0.1) in a Winsock call, the virtual loopback feature simply replaces 127.0.0.1 with 127.X.X.X, where X.X.X is a representation of the session ID + 1. For example, a session ID of 7 is 127.0.0.8. In the unlikely event that the session ID exceeds the fourth octet (more than 255), the address rolls over to the next octet (127.0.1.0), to the maximum of 127.255.255.255.

A process requires virtual loopback in either of the following cases:
- The process uses the Windows socket loopback (localhost) address (127.0.0.1)
- The process uses a hard-coded TCP port number

Use the virtual loopback policy settings for applications that use a loopback address for interprocess communication. No additional configuration is required. Virtual loopback has no dependency on Virtual IP, so you do not have to configure the Microsoft server.
- Virtual IP loopback support. When enabled, this policy setting allows each session to have its own virtual loopback address. This setting is disabled by default. The feature applies only to applications specified with the Virtual IP virtual loopback programs list policy setting.
- Virtual IP virtual loopback programs list. This policy setting specifies the applications that use the virtual IP loopback feature. This setting applies only when the Virtual IP loopback support policy setting is enabled.

Related feature

You can use the following registry settings to ensure that virtual loopback is given preference over virtual IP; this is called preferred loopback. However, proceed with caution:
- Preferred loopback is supported on Windows 2008 R2 only.

- Use preferred loopback only if both Virtual IP and virtual loopback are enabled; otherwise, you may have unintended results.
- Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Run regedit on the servers where the applications reside.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP for 32-bit machines)
- Name: PreferLoopback, Type: REG_DWORD, Data: 1
- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: <list of processes>

Secondary database locations

Sep 09, 2015

By default, the Configuration Logging and Monitoring databases (the secondary databases) are located on the same server as the Site Configuration database. Initially, all three databases have the same name. Citrix recommends that you change the location of the secondary databases after you create a Site. You can host the Configuration Logging and Monitoring databases on the same server or on different servers. The backup strategy for each database may differ.

When you change the location of the Configuration Logging or Monitoring database:

- The data in the previous database is not imported to the new database.
- Logs cannot be aggregated from both databases when retrieving logs.
- The first log entry in the new database indicates that a database change occurred, but it does not identify the previous database.

Before you change the location of the Configuration Logging or Monitoring database, install a supported version of Microsoft SQL Server on the server where the database will reside. Set up mirror, cluster, or other supported redundancy infrastructures, as needed.

You cannot change the location of the Configuration Logging database when mandatory logging is enabled.

Note: You cannot use this method to change the location of the Site Configuration database.

1. Select Configuration in the Studio navigation pane. The names and addresses of the three databases are listed, plus mirror server addresses, if configured.
2. Select the database for which you want to specify a new location and then select Change Database in the Actions pane.
3. Specify the location of the server containing the new SQL Server installation (using one of the forms in the following table) and the database name.

Database type	What to enter	With this database configuration
Standalone or mirror	servername	The default instance is used and SQL Server uses the default port.
	Servername\INSTANCENAME	A named instance is used and SQL Server uses the default port.
	servername,port-number	The default instance is used and SQL Server uses a custom port. (The comma is required.)
Other	cluster-name	A clustered database.
	availability-group-listener	An Always-On database.

4. If you want Studio to create the database, click OK. When prompted, click OK, and Studio will create the database automatically. Studio attempts to access the database using the current Studio user's credentials; if that fails, you are prompted for the database user's credentials. Studio then uploads the database schema to the database. (The credentials are retained only for the database creation time frame.)

5. If you want to create the database manually, click Generate script. The generated scripts includes instructions for manually creating the database and a mirror database, if needed. Ensure that the database is empty and that at least one user has permission to access and change the database before uploading the schema.

Delivery Controller environment

Jul 16, 2014

In a deployment, the Delivery Controller is the server-side component that is responsible for managing user access, plus brokering and optimizing connections. Controllers also provide the Machine Creation Services that create desktop and server images.

A Site must have at least one Delivery Controller. After you install the initial Controller and create a Site, you can add additional Controllers. There are two primary benefits from having more than one Controller in a Site.

- Redundancy — As best practice, a production Site should always have at least two Controllers on different physical servers. If one Controller fails, the others can manage connections and administer the Site.
- Scalability — As Site activity grows, so does CPU utilization on the Controller and SQL Server database activity. Additional Controllers provide the ability to handle more users and more applications and desktop requests, and can improve overall responsiveness.

How Virtual Delivery Agents (VDAs) discover Controllers

Before a VDA can be used, it must register (establish communication) with a Controller on the Site. The VDA finds a Controller by checking a list of Controllers called the ListofDDCs. The ListOfDDCs comprises one or more DNS entries or IP addresses that point the VDA to Controllers on the Site. For load balancing, the VDA automatically distributes connections across all Controllers in the list.

In addition to the ListOfDDCs, the ListOfSIDs indicates which machine Security IDs (SIDs) the VDA allows to contact it as a Controller. The ListOfSIDs can be used to decrease the load on Active Directory or to avoid possible security threats from a compromised DNS server.

It is important to ensure that the ListOfDDCs and ListOfSIDs on all VDAs contain current information as Controllers are added and removed in the Site. If the lists are not updated, a VDA might reject session launches that were brokered by an unlisted Controller. Invalid entries can delay the startup of the virtual desktop system software. To keep the lists current, you can:

- Use the auto-update feature, which automatically updates the ListOfDDCs and ListOfSIDs as Controllers are added or removed. By default, auto-update is enabled.
- Self-manage – that is, manually update policy or registry settings that identify Controllers.

Information in the ListOfDDCs and ListOfSIDs can come from several places in a deployment. The VDA checks the following locations, in order, stopping at the first place it finds the lists:

1. A persistent storage location maintained for the auto-update feature. This location contains Controller information when auto-update is enabled and after the VDA successfully registers for the first time after installation. (This storage also holds machine policy information, which ensures that policy settings are retained across restarts.)
   For its initial registration after installation, or when auto-update is disabled, the VDA checks the following locations.
2. Policy settings (Controllers, Controller SIDs).
3. The Controller information under the Virtual Desktop Agent key in the registry. The VDA installer initially populates these values, based on Controller information you specify when installing the VDA.
4. OU-based Controller discovery. This is a legacy method maintained for backward compatibility.
5. The Personality.ini file created by Machine Creation Services.

If a ListOfDDCs specifies more than one Controller, the VDA attempts to connect to them in random order. The

ListOfDDCs can also contain Controller groups, which are designated by brackets surrounding two or more Controller entries. The VDA attempts to connect to each Controller in a group before moving to other entries in the ListOfDDCs.

For XenDesktop users who have upgraded from versions earlier than 7.0, the auto-update feature replaces the CNAME function from the earlier version. You can manually re-enable the CNAME function, if desired; however, for DNS aliasing to work consistently, you cannot use both the auto-update feature and the CNAME function. See CTX137960 for information about re-enabling the CNAME functionality.

Considerations for choosing auto-update or self-manage

The policy setting that enables/disables auto-update is enabled by default.

The following types of deployments cannot use auto-update, and must self-manage.

- Deployments that use Controller groups.
- Deployments that use ListOfSIDs for security reasons. (Deployments that use ListOfSIDs to decrease the Active Directory load can use auto-update.)
- Deployments that use Provisioning Services without a write-back disk.
- Deployments that use the Controllers or Controller SIDs policy setting.

Use auto-update

The auto-update policy setting is located in the Virtual Delivery Agent category.

- To enable auto-update, enable the Enable auto update of Controllers policy setting. This setting is enabled by default.
- To disable auto-update, disable the Enable auto update of Controllers policy setting.

When auto-update is enabled and you install a VDA, the VDA attempts to register with one of the Controller values you specified when you installed the VDA. The installer writes the Controller information you specify during VDA installation to the ListOfDDCs registry value.

After the VDA registers, the Controller with which it registered sends a list of the current Controller Fully Qualified Domain Names (FQDNs) and Security IDs (SIDs) to the VDA. The VDA writes this list to the auto-update persistent storage. Each Controller also checks the Site Configuration Database every 90 minutes for Controller information – if a Controller has been added or removed since the last check, or if a policy change has occurred, the Controller sends updated lists to its registered VDAs. The VDA will accept connections from all the Controllers in the most recent list it received.

If a VDA receives a list that does not include the Controller it is registered with (in other words, that Controller was removed from the Site), the VDA re-registers, choosing among the Controllers in the list. After a VDA registers or re-registers, it receives an updated list.

For example:

1. A deployment has three Controllers: A, B, and C. A VDA is installed and registers with Controller B (which was specified during VDA installation).
2. Two Controllers (D and E) are added to the Site. Within 90 minutes, VDAs receive updated lists and will accept connections from Controllers A, B, C, D, and E. (The load will not be spread equally to all Controllers until the VDAs are restarted.)
3. Controller B is removed from the Site. Within 90 minutes, VDAs receive updated lists because there has been a Controller change since the last check. The VDA installed in step 1 is registered with Controller B, which is no longer on the list, so that VDA re-registers, choosing among the Controllers in the current list (A, C, D, and E).

Self-manage

If you do not use auto-update, you must update the Citrix policy setting or registry values for each Virtual Delivery Agent (VDA) in the site (or the VDA image) after you add, move, or remove Delivery Controllers in the Site. Registry changes can also be updated using Group Policy Object.

To self-manage using Citrix policy settings:

1. Update the FQDN values specified in the Controllers policy setting. This policy setting is located in the Virtual Delivery Agent category.
2. If you also use ListOfSIDs in your deployment, update the SID values specified in the Controller SIDs policy setting.

To self-manage using the registry:

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Update the ListOfDDCs registry key, which lists the FQDNs of all the Controllers in the Site. (This key is the equivalent of the Active Directory Site OU.) Separate multiple values with spaces. Surround Controller groups with brackets.
   HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)
   If the HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent registry location contains both the ListOfDDCs and FarmGUID keys, ListOfDDCs is used for Controller discovery; FarmGUID is present if a site OU was specified during VDA installation.

2. Optionally, update the ListOfSIDs registry key:
   HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

Add, remove, or move Controllers, or move a VDA

Mar 23, 2015

To add, remove, or move a Delivery Controller, you need the following roles or permissions:

Operation	Purpose	Server role	Database role
Database creation	Create suitable empty database	dbcreator	
Schema creation	Create all service-specific schemas and add first Controller to Site	securityadmin *	db_owner
Add Controller	Add Controller (other than the first) to the Site	securityadmin *	db_owner
Add Controller (mirror server)	Add Controller login to the database server currently in the mirror role of a mirrored database	securityadmin *	
Remove Controller	Remove Controller from the Site		db_owner
Schema update	Apply schema updates or hotfixes		db_owner

* While technically more restrictive, in practice, the securityadmin server role should be treated as equivalent to the sysadmin server role.

When using Studio to perform these operations, the user account must explicitly be a member of the sysadmin server role.

If your deployment uses database mirroring:

- Before adding, removing, or moving a Controller, ensure that the principal and mirrored databases are both running. In addition, if you are using scripts with SQL Server Management Studio, enable SQLCMD mode before executing the scripts.
- To verify mirroring after adding, removing, or moving a Controller, run the get-configdbconnection PowerShell cmdlet to ensure that the Failover Partner has been set in the connection string to the mirror.

After you add, remove, or move a Controller:

- If auto-update is enabled, the Virtual Delivery Agents (VDAs) will receive an updated list of Controllers within 90 minutes.
- If auto-update is not enabled, ensure that the Controller policy setting or ListOfDDCs registry key are updated for all VDAs. After moving a Controller to another Site, update the policy setting or registry key on both Sites.

Add a Controller

You cannot add servers installed with an earlier version of this software to a Site that was created with this version.

1. On the server you want to add, run the installer and select the Delivery Controller and any other core components you want to install.
2. In Studio, click Join existing deployment and enter the Site address.

Remove a Controller

Removing a Controller does not uninstall the Citrix software or any other component; it removes the Controller from the Database so that it can no longer be used to broker connections and perform other tasks. If you remove a Controller, you can later add it back to the same Site or to another Site. A Site requires at least one Controller, so you cannot remove the last one listed in Studio.

Note: Make sure that the Controller is powered on so that Studio loads in less than one hour. Once Studio loads the Controller you want to remove, power off the Controller when prompted to do so.
When you remove a Controller from a Site, the Controller logon to the database server is not removed. This avoids potentially removing a logon that is used by other products' services on the same machine. The logon must be removed manually if it is no longer required; the securityadmin server role permission is needed to remove the logon.

Important: Do not remove the Controller from Active Directory until *after* you remove it from the Site.

1. Select Configuration > Controllers in the Studio navigation pane, then select the Controller you want to remove.
2. Select Remove Controller in the Actions pane. If you do not have the correct database roles and permissions, you are offered the option of generating a script that allows your database administrator to remove the Controller for you.
3. You might need to remove the Controller's machine account from the database server. Before doing this, check that another service is not using the account.

After using Studio to remove a Controller, traffic to that Controller might linger for a short amount of time to ensure proper completion of current tasks. If you want to force the removal of a Controller in a very short time, Citrix recommends you shut down the server where it was installed, or remove that server from Active Directory. Then, restart the other Controllers on the Site to ensure no further communication with the removed Controller.

Move a Controller to another Site

You cannot move a Controller to a Site that was created with an earlier version of this software.
1. On the Site where the Controller is currently located (the old Site), select Configuration > Controllers in the Studio navigation pane, then select the Controller you want to move.
2. Select Remove Controller in the Actions pane. If you do not have the correct database roles and permissions, you are offered the option of generating a script that allows your database administrator to remove the Controller for you. A Site requires at least one Controller, so you cannot remove the last one listed in Studio.
3. On the Controller you are moving, open Studio, reset the services when prompted, select Join existing site, and enter the address of the new Site.

Move a VDA to another Site

If a VDA was provisioned using Provisioning Services or is an existing image, you can move a VDA to another Site (from Site 1 to Site 2) when upgrading, or when moving a VDA image that was created in a test Site to a production Site. VDAs provisioned using Machine Creation Services (MCS) cannot be moved from one Site to another because MCS does not support changing the ListOfDDCs a VDA checks to register with a Controller; VDAs provisioned using MCS always check the ListOfDDCs associated with the Site in which they were created.

There are two ways to move a VDA to another site: using the installer or Citrix policies.
- Installer: Run the installer and add a Controller, specifying the FQDN (DNS entry) of a Controller in Site 2.
  Important: Specify Controllers in the installer only when the Controllers policy setting is not used.
- Group Policy Editor: The following example moves multiple VDAs between Sites.
  1. Create a policy in Site 1 that contains the following settings, then filter the policy to the Delivery Group level to

initiate a staged VDA migration between the Sites.

- Controllers - containing FQDNs (DNS entries) of one or more Controllers in Site 2.
- Enable auto update of Controllers - set to disabled.

2. Each VDA in the Delivery Group is alerted within 90 minutes of the new policy. The VDA ignores the list of Controllers it receives (because auto-update is disabled); it selects one of the Controllers specified in the policy, which lists the Controllers in Site 2.
3. When the VDA successfully registers with a Controller in Site 2, it receives the Site 2 ListOfDDCs and policy information, which has auto-update enabled by default. Since the Controller with which the VDA was registered in Site 1 is not on the list sent by the Controller in Site 2, the VDA re-registers, choosing among the Controllers in the Site 2 list. From then on, the VDA is automatically updated with information from Site 2.

Active Directory OU-based Controller discovery

Aug 31, 2016

This Delivery Controller discovery method is supported primarily for backward compatibility, and is valid only for Virtual Delivery Agents (VDAs) for Windows Desktop OS, not VDAs for Windows Server OS. Active Directory-based discovery requires that all computers in a Site are members of a domain, with mutual trusting relationships between the domain used by the Controller and the domain(s) used by desktops. If you use this method, you must configure the GUID of the OU in each desktop registry.

To perform an OU-based Controller discovery, run the Set-ADControllerDiscovery.ps1 PowerShell script on the Controller (each Controller contains this script in the folder $Env:ProgramFiles\Citrix\Broker\Service\Setup Scripts). To run the script, you must have CreateChild permissions on a parent OU, plus full administration rights.

When you create a Site, a corresponding Organizational Unit (OU) must be created in Active Directory if you want desktops to discover the Controllers in the Site through Active Directory. The OU can be created in any domain in the forest that contains your computers. As best practice, the OU should also contain the Controllers in the Site, but this is not enforced or required. A domain administrator with appropriate privileges can create the OU as an empty container, then delegate administrative authority over the OU to a Citrix administrator.

The script creates several essential objects. Only standard Active Directory objects are created and used. It is not necessary to extend the schema.

- A Controllers security group. The computer account of all Controllers in the Site must be a member of this security group. Desktops in a Site accept data from Controllers only if they are members of this security group.
  Ensure that all Controllers have the 'Access this computer from the network' privilege on all virtual desktops running the VDA. You can do this by giving the Controllers security group this privilege. If Controllers do not have this privilege, VDAs will not register.

- A Service Connection Point (SCP) object that contains information about the Site, such as the Site name. If you use the Active Directory Users and Computers administrative tool to inspect a Site OU, you might need to enable Advanced Features in the View menu to see SCP objects.
- A container called RegistrationServices, which is created in the Site OU. This contains one SCP object for each Controller in the Site. Each time the Controller starts, it validates the contents of its SCP and updates it, if necessary.

If multiple administrators are likely to add and remove Controllers after the initial installation, they need permissions to create and delete children on the RegistrationServices container, and Write properties on the Controllers security group; these permissions are granted automatically to the administrator who runs the Set-ADControllerDiscovery.ps1 script. The domain administrator or the original installing administrator can grant these permissions, and Citrix recommends setting up a security group to do this.

When you are using a Site OU:

- Information is written to Active Directory only when installing or uninstalling this software, or when a Controller starts and needs to update the information in its SCP (for example, because the Controller was renamed or because the communication port was changed). By default, the Set-ADControllerDiscovery.ps1 script sets up permissions on the objects in the Site OU appropriately, giving each Controller Write access to its SCP. The contents of the objects in the Site OU are used to establish trust between desktops and Controllers. Ensure that:
  - Only authorized administrators can add or remove computers from the Controllers security group, using the security group's access control list (ACL).

- Only authorized administrators and the respective Controller can change the information in the controller's SCP.
- If your deployment uses replication, be aware of potential delays; see the Microsoft documentation for details. This is particularly important if you create the Site OU in a domain that has domain controllers in multiple Active Directory sites. Depending on the location of desktops, Controllers, and domain controllers, changes that are made to Active Directory when you are initially creating the Site OU, installing or uninstalling Controllers, or changing Controller names or communication ports might not be visible to desktops until that information is replicated to the appropriate domain controller. The symptoms of such replication delay include desktops that cannot establish contact with Controllers and are therefore not available for user connections.
- This software uses several standard computer object attributes in Active Directory to manage desktops. Depending on your deployment, the machine object's fully qualified domain name, as stored in the desktop's Active Directory record, can be included as part of the connection settings that are returned to the user to make a connection. Ensure that this information is consistent with information in your DNS environment.

Permissions summary

To create a Site, the Citrix administrator who runs the script must have rights over the Site OU to create objects (SCP, container, and security group).

> (If the Site OU is not present, the administrator must have rights to create that as well. Citrix recommends that the AD domain administrator pre-create that OU and delegate rights to it to the Citrix Site administrator identity. Optionally, the script can also create the Site OU. To allow this, the administrator needs the “create OU” right on the new OU’s parent OU. However, as noted, Citrix does not recommend this.)

Later, to add or remove a Controller from the Site, the Citrix administrator must have rights to add/remove a machine from the security group, and create/delete an SCP.

During normal operations, Controllers and VDAs need read rights to all objects in the OU and below. VDAs access the OU as their own machine identity; that machine identity needs at least read rights in the OU to be able to discover Controllers. A Controller also needs the rights to set properties on its own SCP object in the container.

Granting the Citrix administrator full rights to the child OUs will permit all these actions. However, if your deployment has stricter security requirements (such as restricting who can use the script for which action), you can use the Delegation of Control wizard to set specific rights. The following example procedure grants rights to create the Site.

1. Create an OU to contain the child objects (Service Connection Point (SCP), container, and security group).
2. Select the OU, then right-click and select **Delegate Control**.
3. In the Delegation of Control wizard, specify the domain user to delegate control to for the OU.
4. On the **Tasks to Delegate** page, select **Create a custom task to delegate**.
5. On the **Active Directory Object type** page, accept the default **This folder, existing objects in this folder, and creation of new objects in this folder**.
6. On the **Permissions** page, select **Permissions Create All Child Objects**.
7. Finish the wizard to confirm the privileges.

To move a Controller to another Site using OU-based Controller discovery

Follow the directions in Move a Controller to another Site. After you remove the Controller from the old Site (step 2), run the PowerShell script Set-ADControllerDiscovery –sync.

This script synchronizes the OU with the current set of Controllers. After joining the existing Site (step 3), run the same script on any Controller in the new Site.

Session management

Sep 09, 2015

Maintaining session activity is critical to providing the best user experience. Losing connectivity due to unreliable networks, highly variable network latency, and range limitations of wireless devices can lead to user frustration. Being able to move quickly between workstations and access the same set of applications each time they log on is a priority for many mobile workers such as health-care workers in a hospital.

Use the following features to optimize the reliability of sessions, reduce inconvenience, downtime, and loss of productivity; using these features, mobile users can roam quickly and easily between devices.

- Session reliability
- Auto Client Reconnect
- ICA Keep-Alive
- Workspace control

Session reliability

Session Reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes.

This feature is especially useful for mobile users with wireless connections. For example, a user with a wireless connection enters a railroad tunnel and momentarily loses connectivity. Ordinarily, the session is disconnected and disappears from the user's screen, and the user has to reconnect to the disconnected session. With Session Reliability, the session remains active on the machine. To indicate that connectivity is lost, the user's display freezes and the cursor changes to a spinning hourglass until connectivity resumes on the other side of the tunnel. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session Reliability reconnects users without reauthentication prompts.

Citrix Receiver users cannot override the Controller setting.

You can use Session Reliability with Secure Sockets Layer (SSL). SSL encrypts only the data sent between the user device and NetScaler Gateway.

Enable and configure Session Reliability with the following policy settings:

- The Session reliability connections policy setting allows or prevents session reliability.
- The Session reliability timeout policy setting has a default of 180 seconds, or three minutes. Although you can extend the amount of time Session Reliability keeps a session open, this feature is designed for user convenience and therefore does not prompt the user for reauthentication. As you extend the amount of time a session is kept open, chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.
- Incoming session reliability connections use port 2598, unless you change the port number in the Session reliability port number policy setting.
- If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, use the Auto Client Reconnect feature. You can configure the Auto client reconnect authentication policy setting to prompt users to reauthenticate when reconnecting to interrupted sessions.
  If you use both Session Reliability and Auto Client Reconnect, the two features work in sequence. Session Reliability closes, or disconnects, the user session after the amount of time you specify in the Session reliability timeout policy setting. After that, the Auto Client Reconnect policy settings take effect, attempting to reconnect the user to the

disconnected session.

Auto Client Reconnect

With the Auto Client Reconnect feature, Receiver can detect unintended disconnections of ICA sessions and reconnect users to the affected sessions automatically. When this feature is enabled on the server, users do not have to reconnect manually to continue working.

For application sessions, Receiver attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For desktop sessions, Receiver attempts to reconnect to the session for a specified period of time, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this period of time is five minutes. To change this period of time, edit this registry on the user device:

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>
where <seconds> is the number of seconds after which no more attempts are made to reconnect the session.

Enable and configure Auto Client Reconnect with the following policy settings:

- Auto client reconnect. Enables or disables automatic reconnection by Receiver after a connection has been interrupted.
- Auto client reconnect authentication. Enables or disables the requirement for user authentication after automatic reconnection.
- Auto client reconnect logging. Enables or disables logging of reconnection events in the event log. Logging is disabled by default. When enabled, the server's system log captures information about successful and failed automatic reconnection events. Each server stores information about reconnection events in its own system log; the site does not provide a combined log of reconnection events for all servers.

Auto Client Reconnect incorporates an authentication mechanism based on encrypted user credentials. When a user initially logs on, the server encrypts and stores the user credentials in memory, and creates and sends a cookie containing the encryption key to Receiver. Receiver submits the key to the server for reconnection. The server decrypts the credentials and submits them to Windows logon for authentication. When cookies expire, users must reauthenticate to reconnect to sessions.

Cookies are not used if you enable the Auto client reconnection authentication setting. Instead, users are presented with a dialog box to users requesting credentials when Receiver attempts to reconnect automatically.

For maximum protection of user credentials and sessions, use SSL encryption for all communication between clients and the Site.

Disable Auto Client Reconnect on Citrix Receiver for Windows by using the icaclient.adm file. For more information, see the documentation for your Receiver for Windows version.

Settings for connections also affect Auto Client Reconnect:

- By default, Auto Client Reconnect is enabled through policy settings at the Site level, as described above. User reauthentication is not required. However, if a server's ICA TCP connection is configured to reset sessions with a broken communication link, automatic reconnection does not occur. Auto Client Reconnect works only if the server disconnects sessions when there is a broken or timed out connection. In this context, the ICA TCP connection refers to a server's virtual port (rather than an actual network connection) that is used for sessions on TCP/IP networks.
- By default, the ICA TCP connection on a server is set to disconnect sessions with broken or timed out connections. Disconnected sessions remain intact in system memory and are available for reconnection by Receiver.

- The connection can be configured to reset or log off sessions with broken or timed-out connections. When a session is reset, attempting to reconnect initiates a new session; rather than restoring a user to the same place in the application in use, the application is restarted.
- If the server is configured to reset sessions, Auto Client Reconnect creates a new session. This process requires users to enter their credentials to log on to the server.
- Automatic reconnection can fail if Receiver or the plug-in submits incorrect authentication information, which might occur during an attack or the server determines that too much time has elapsed since it detected the broken connection.

ICA Keep-Alive

Enabling the ICA Keep-Alive feature prevents broken connections from being disconnected. When enabled, if the server detects no activity (for example, no clock change, no mouse movement, no screen updates), this feature prevents Remote Desktop Services from disconnecting that session. The server sends keep-alive packets every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

Note: ICA Keep-Alive works only if you are not using Session Reliability. Session Reliability has its own mechanisms to prevent broken connections from being disconnected. Configure ICA Keep-Alive only for connections that do not use Session Reliability.
ICA Keep-Alive settings override keep-alive settings that are configured in Microsoft Windows Group Policy.

Enable and configure ICA Keep-Alive with the following policy settings:
- ICA keep alive timeout. Specifies the interval (1-3600 seconds) used to send ICA keep-alive messages. Do not configure this option if you want your network monitoring software to close inactive connections in environments where broken connections are so infrequent that allowing users to reconnect to sessions is not a concern.
  The default interval is 60 seconds: ICA Keep-Alive packets are sent to user devices every 60 seconds. If a user device does not respond in 60 seconds, the status of the ICA sessions changes to disconnected.

- ICA keep alives. Sends or prevents sending ICA keep-alive messages.

Workspace control

Workspace control lets desktops and applications follow a user from one device to another. This ability to roam enables a user to access all desktops or open applications from anywhere simply by logging on, without having to restart the desktops or applications on each device. For example, workspace control can assist health-care workers in a hospital who need to move quickly among different workstations and access the same set of applications each time they log on. If you configure workspace control options to allow it, these workers can disconnect from multiple applications at one client device and then reconnect to open the same applications at a different client device.

Workspace control affects the following activities:
- **Logging on –** By default, workspace control enables users to reconnect automatically to all running desktops and applications when logging on, bypassing the need to reopen them manually. Through workspace control, users can open disconnected desktops or applications, as well as any that are active on another client device. Disconnecting from a desktop or application leaves it running on the server. If you have roaming users who need to keep some desktops or applications running on one client device while they reconnect to a subset of their desktops or applications on another client device, you can configure the logon reconnection behavior to open only the desktops or applications that the user disconnected from previously.
- **Reconnecting –** After logging on to the server, users can reconnect to all of their desktops or applications at any time by clicking Reconnect. By default, Reconnect opens desktops or applications that are disconnected, plus any that are currently running on another client device. You can configure Reconnect to open only those desktops or applications

that the user disconnected from previously.

- **Logging off –** For users opening desktops or applications through StoreFront, you can configure the Log Off command to log the user off from StoreFront and all active sessions together, or log off from StoreFront only.
- **Disconnecting –** Users can disconnect from all running desktops and applications at once, without needing to disconnect from each individually.

Workspace control is available only for Receiver users who access desktops and applications through a Citrix StoreFront connection. By default, workspace control is disabled for virtual desktop sessions, but is enabled for hosted applications. Session sharing does not occur by default between published desktops and any published applications running inside those desktops.

User policies, client drive mappings, and printer configurations change appropriately when a user moves to a new client device. Policies and mappings are applied according to the client device where the user is currently logged on to the session. For example, if a health care worker logs off from a client device in the emergency room of a hospital and then logs on to a workstation in the hospital's X-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect at the session startup.

You can customize which printers appear to users when they change locations. You can also control whether users can print to local printers, how much bandwidth is consumed when users connect remotely, and other aspects of their printing experiences.

For information about enabling and configuring workspace control for users, see the StoreFront documentation.

Using Search in Studio

Sep 09, 2015

Use the Search feature to view information about specific machines, sessions, machine catalogs, applications, or Delivery Groups.

1. Select Search in the Studio navigation pane.
   Note: You cannot search within the machine catalogs or Delivery Groups tabs using the Search box. Use the Search node in the navigation pane.
   To display additional search criteria in the display, click the plus sign next to the Search drop-down fields. Remove search criteria by clicking the minus button.
2. Enter the name or use the drop-down list to select another search option for the item you want to find.
3. Optionally, save your search by selecting Save as. The search appears in the Saved searches list.

Alternatively, click the Expand Search icon (dual downward angle brackets) to display a drop-down list of search properties; you can perform an advanced search by building an expression from the properties in the drop-down list.

Tips to enhance a search:

- To display additional characteristics to include in the display on which you can search and sort, right click any column and select Select columns.
- To locate a user device connected to a machine, use Client (IP) and Is, and enter the device IP address.
- To locate active sessions, use Session State, Is, and Connected.
- To list all of the machines in a Delivery Group, select Delivery Groups in the navigation pane, then select the group, and then select View Machines in the Actions pane.

IPv4/IPv6 support

Sep 09, 2015

This release supports pure IPv4, pure IPv6, and dual-stack deployments that use overlapping IPv4 and IPv6 networks.

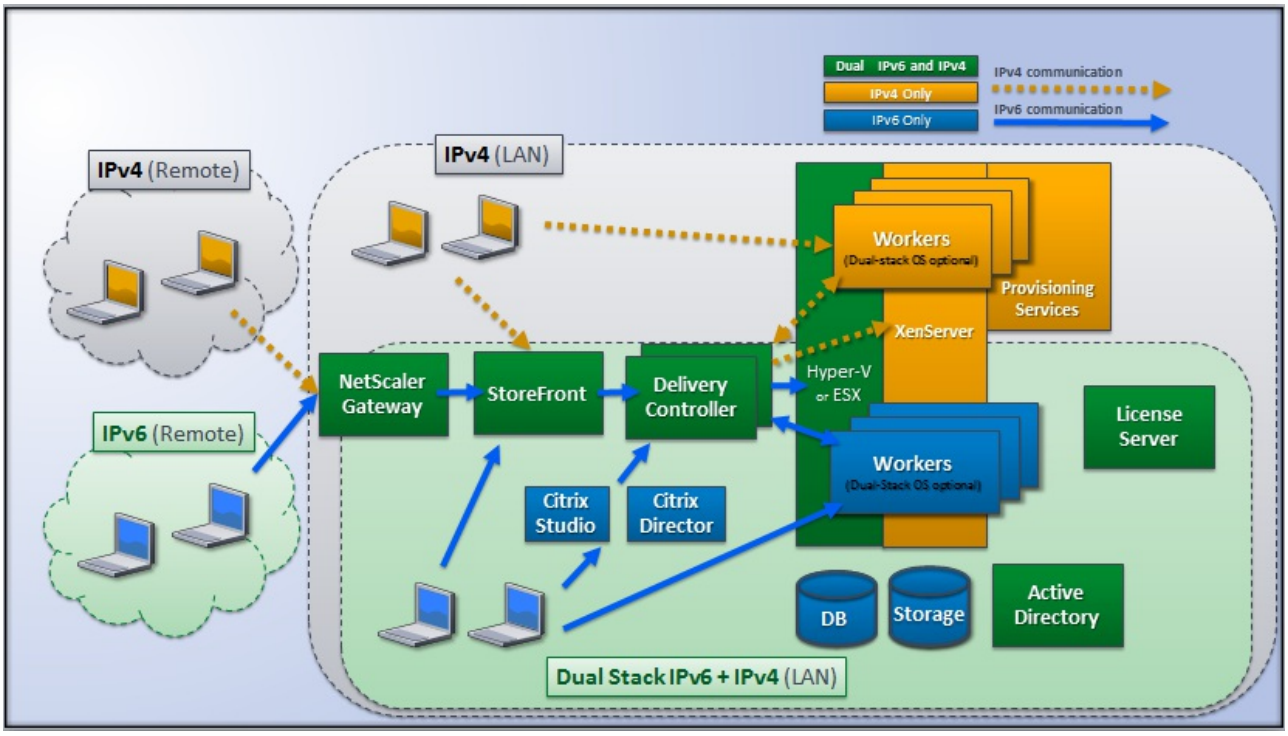
IPv6 communications are controlled with two Virtual Delivery Agent (VDA) connection-related Citrix policy settings:

- A primary setting that enforces the use of IPv6: Only use IPv6 Controller registration.
- A dependent setting that defines an IPv6 netmask: Controller registration IPv6 netmask.

When the Only use IPv6 Controller registration policy setting is enabled, VDAs register with a Delivery Controller for incoming connections using an IPv6 address.

Dual-stack IPv4/IPv6 deployment

The following figure illustrates a dual-stack IPv4/IPv6 deployment. In this scenario, a worker is a VDA installed on a hypervisor or on a physical system, and is used primarily to enable connections for applications and desktops. Components that support dual IPv6 and IPv4 are running on operating systems that use tunneling or dual protocol software.



These Citrix products, components, and features support only IPv4:

- Provisioning Services
- XenServer Version 6.x
- VDAs not controlled by the Only use IPv6 Controller registration policy setting
- XenApp versions earlier than 7.5, XenDesktop versions earlier than 7, and EdgeSight

In this deployment:

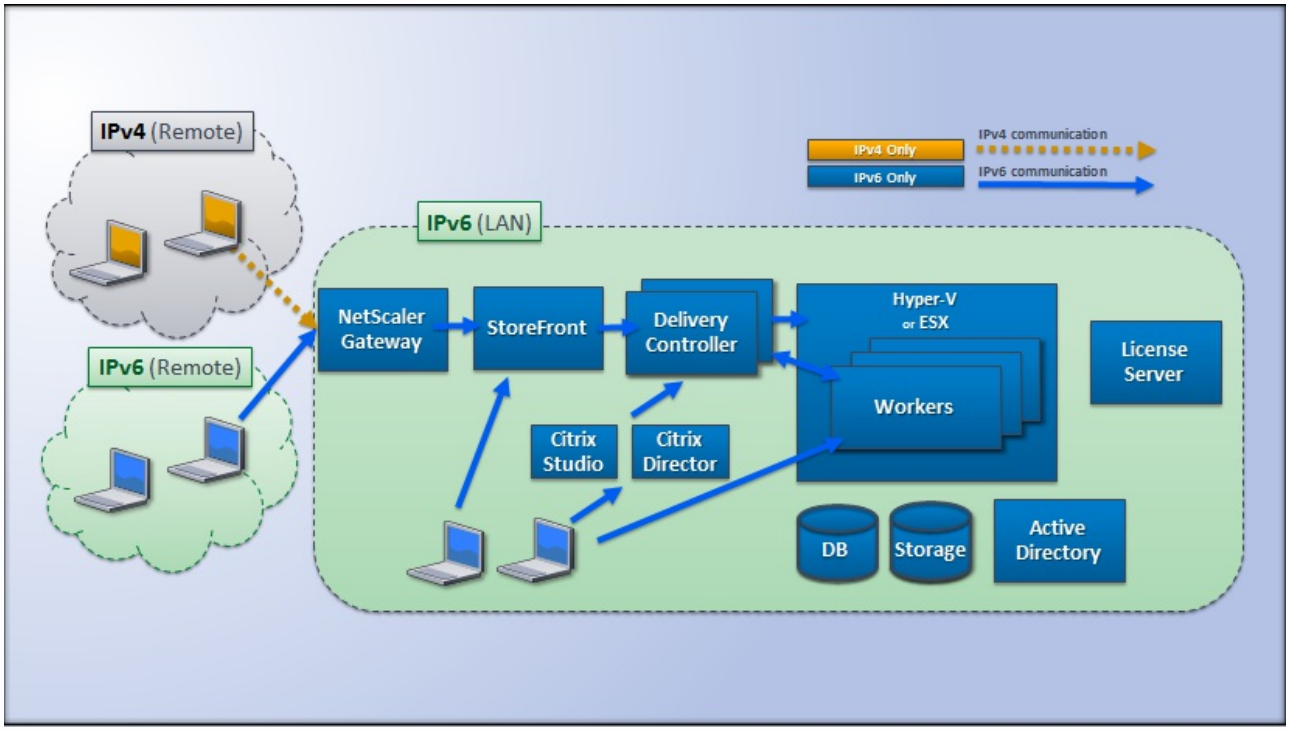
- If a team frequently uses an IPv6 network and the administrator wants them to use IPv6 traffic, the administrator will publish IPv6 desktops and applications for those users based on a worker image or Organizational Unit (OU) that has the primary IPv6 policy setting turned on (that is, Only use IPv6 Controller registration is enabled).
- If a team frequently uses an IPv4 network, the administrator will publish IPv4 desktops and applications for those users

based on a worker image or OU that has the primary IPv6 policy setting turned off (that is, Only use IPv6 Controller registration is disabled), which is the default.

Pure IPv6 deployment

The following figure illustrates a pure IPv6 deployment. In this scenario:

- The components are running on operating systems configured to support an IPv6 network.
- The primary Citrix policy setting (Only use IPv6 Controller registration) is enabled for all VDAs; they must register with the Controller using an IPv6 address.



Policy settings for IPv6

Two Citrix policy settings affect support for a pure IPv6 or dual stack IPv4/IPv6 implementation. Configure the following connection-related policy settings:

- Only use IPv6 Controller registration — Controls which form of address the Virtual Delivery Agent (VDA) uses to register with the Delivery Controller. Default = Disabled
  - When the VDA communicates with the Controller, it uses a single IPv6 address chosen in the following precedence: global IP address, Unique Local Address (ULA), link-local address (only if no other IPv6 addresses are available).
  - When disabled, the VDA registers and communicates with the Controller using the machine's IPv4 address.
- Controller registration IPv6 netmask — A machine can have multiple IPv6 addresses; this policy setting allows administrators to restrict the VDA to only a preferred subnet (rather than a global IP, if one is registered). This setting specifies the network where the VDA will register: the VDA registers only on the first address that matches the specified netmask. This setting is valid only if the Only use IPv6 Controller registration policy setting is enabled. Default = Empty string

Important: Important: Use of IPv4 or IPv6 by a VDA is determined solely by these policy settings. In other words, to use IPv6 addressing, the VDA must be controlled by a Citrix policy with the Only use IPv6 Controller registration setting enabled.

Deployment considerations

If your environment contains both IPv4 and IPv6 networks, you will need separate Delivery Group configurations for the IPv4-only clients and for the clients who can access the IPv6 network. Consider using naming, manual Active Directory

group assignment, or Smart Access filters to differentiate users.

Reconnection to a session may fail if the connection is initiated on an IPv6 network, and then attempts are made to connect again from an internal client that has only IPv4 access.

Client folder redirection

Jan 29, 2016

Client folder redirection changes the way client-side files are accessible on the host-side session. When you enable only client drive mapping on the host-side, client-side full volumes are automatically mapped to the sessions as Universal Naming Convention (UNC) links. When you enable client folder redirection on the host-side and the user configures it on the user device, the portion of the local volume specified by the user is redirected.

Only the user-specified folders appear as UNC links inside sessions instead of the complete file system on the user device. If you disable UNC links through the registry, client folders appear as mapped drives inside the session.

Client folder redirection is supported on Windows Desktop OS machines only.

Client folder redirection for an external USB drive will not be saved on detaching and reattaching the device.

Enable client folder direction on the host-side. Then, on the client device, specify which folders to redirect (the application you use to specify the client folder options is included with the Citrix Receiver supplied with this release.
Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. On the host-side:
    1. Create a key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
    2. Create a REG_DWORD value.
        - Name: CFROnlyModeAvailable
        - Type: REG_DWORD
        - Data: Set to 1
2. On the user device:
    1. Ensure the latest version of Receiver is installed.
    2. From the Receiver installation directory, start CtxCFRUI.exe.
    3. Select the Custom radio button and add, edit, or remove folders.
    4. Disconnect and reconnect your sessions for the setting to take effect.

Personal vDisk 7.x

Sep 29, 2015

The personal vDisk feature retains the single image management of pooled and streamed desktops while allowing users to install applications and change their desktop settings. Unlike traditional Virtual Desktop Infrastructure (VDI) deployments involving pooled desktops, where users lose their customization and personal applications when the administrator changes the master image, deployments using personal vDisks retain those changes. This means administrators can easily and centrally manage their master images while providing users with a customized and personalized desktop experience.

Personal vDisks provide this separation by redirecting all changes made on the user's VM to a separate disk (the personal vDisk), which is attached to the user's VM. The content of the personal vDisk is blended at runtime with the content from the master image to provide a unified experience. In this way, users can still access applications provisioned by their administrator in the master image.

Personal vDisks have two parts, which use different drive letters and are by default equally sized:

- User profile - This contains user data, documents, and the user profile. By default this uses drive P: but you can choose a different drive letter when you create a catalog with machines using personal vDisks. The drive used also depends on the EnableUserProfileRedirection setting.
- Virtual Hard Disk (.vhd) file - This contains all other items, for example applications installed in C:\Program Files. This part is not displayed in Windows Explorer and, since Version 5.6.7, does not require a drive letter.

Personal vDisks support the provisioning of department-level applications, as well as applications downloaded and installed by users, including those that require drivers (except phase 1 drivers), databases, and machine management software. If a user's change conflicts with an administrator's change, the personal vDisk provides a simple and automatic way to reconcile the changes.

In addition, locally administered applications (such as those provisioned and managed by local IT departments) can also be provisioned into the user's environment. The user experiences no difference in usability; personal vDisks ensure all changes made and all applications installed are stored on the vDisk. Where an application on a personal vDisk exactly matches one on a master image, the copy on the personal vDisk is discarded to save space without the user losing access to the application.

Physically, you store personal vDisks on the hypervisor but they do not have to be in the same location as other disks attached to the virtual desktop. This can lower the cost of personal vDisk storage.

During Site creation, when you create a connection, you define storage locations for disks that are used by VMs. You can separate the Personal vDisks from the disks used by the operating system. Each VM must have access to a storage location for both disks. If you use local storage for both, they must be accessible from the same hypervisor. To ensure this requirement is met, Studio offers only compatible storage locations. Later, you can also add personal vDisks and storage for them to existing hosts (but not machine catalogs) from Configuration > Hosting in Studio.

Back up personal vDisks regularly using any preferred method. The vDisks are standard volumes in a hypervisor's storage tier, so you can back them up, just like any other volume.

What's new in personal vDisk 7.6.1

The following improvements are included in this release:

- This version of personal vDisk contains performance improvements that reduce the amount of time it takes to apply an

image update to a personal vDisk catalog.

The following known issues are fixed in this release:

- Attempting an in-place upgrade of a base virtual machine from Microsoft Office 2010 to Microsoft Office 2013 resulted in the user seeing a reconfiguration window followed by an error message; "Error 25004. The product key you entered cannot be used on this machine." In the past, it was recommended that Office 2010 be uninstalled in the base virtual machine before installing Office 2013. Now, it is no longer necessary to uninstall Office 2010 when performing an in-place upgrade to the base virtual machine (#391225).
- During the image update process, if a higher version of Microsoft .Net exists on the users personal vDisk, it was overwritten by a lower version from the base image. This caused issues for users running certain applications installed on their personal vDisk which required the higher version, such as Visual Studio (#439009).
- A Provisioning Services imaged disk with personal vDisk install and enabled, cannot be used to create a non-personal vdisk machine catalog. This restriction has been removed (#485189).

About Personal vDisk 7.6

New in version 7.6:

- Improved personal vDisk error handling and reporting. In Studio, when you display PvD-enabled machines in a catalog, a "PvD" tab provides monitoring status during image updates, plus estimated completion time and progress. Enhanced state displays are also provided.
- A personal vDisk Image Update Monitoring Tool for earlier releases is available from the ISO media (ISO\Support\Tools\Scripts\PvdTool). Monitoring capabilities are supported for previous releases, however the reporting capabilities will not be as robust compared to the current release.
- Provisioning Services test mode allows you to boot machines with an updated image in a test catalog. After you verify its stability, you can promote the test version of the personal vDisk to production.
- A new feature enables you to calculate the delta between two inventories during an inventory, instead of calculating it for each PvD desktop. New commands are provided to export and import a previous inventory for MCS catalogs. (Provisioning Services master vDisks already have the previous inventory.)

Known issues from 7.1.3 fixed in version 7.6:

- Interrupting a personal vDisk installation upgrade can result in corrupting an existing personal vDisk installation. [#424878]
- A virtual desktop may become unresponsive if the personal vDisk runs for an extended period of time and a non-page memory leak occurs. [#473170]

New known issues in version 7.6:

- The presence of antivirus products can affect how long it takes to run the inventory or perform an update. Performance can improve if you add CtxPvD.exe and CtxPvDSvc.exe to the PROCESS exclusion list of your antivirus product. These files are located in C:\Program Files\Citrix\personal vDisk\bin. [#326735]
- Hard links between files inherited from the master image are not preserved in personal vDisk catalogs. [#368678]
- After upgrading from Office 2010 to 2013 on the Personal vDisk master image, Office might fail to launch on virtual machines because the Office KMS licensing product key was removed during the upgrade. As a workaround, uninstall Office 2010 and reinstall Office 2013 on the master image. [#391225]
- Personal vDisk catalogs do not support VMware Paravirtual SCSI (PVSCSI) controllers. To prevent this issue, use the default controller. [#394039]
- For virtual desktops that were created with Personal vDisk version 5.6.0 and are upgraded to 7, users who logged on to the master virtual machine (VM) previously might not find all their files in their pooled VM. This issue occurs because a new user profile is created when they log on to their pooled VM. There is no workaround for this issue. [#392459]

- Personal vDisks running Windows 7 cannot use the Backup and Restore feature when the Windows system protection feature is enabled. If system protection is disabled, the user profile is backed up, but the userdata.v2.vhd file is not. Citrix recommends disabling system protection and using Backup and Restore to back up the user profile. [#360582]
- When you create a VHD file on the base VM using the Disk Management tool, you might be unable to mount the VHD. As a workaround, copy the VHD to the PvD volume. [#355576]
- Office 2010 shortcuts remain on virtual desktops after this software is removed. To work around this issue, delete the shortcuts. [#402889]
- When using Microsoft Hyper-V, you cannot create a catalog of machines with personal vDisks when the machines are stored locally and the vDisks are stored on Cluster Shared Volumes (CSVs); catalog creation fails with an error. To work around this issue, use an alternative storage setup for the vDisks. [#423969]
- When you log on for the first time to a virtual desktop that is created from a Provisioning Services catalog, the desktop prompts for a restart if the personal vDisk has been reset (using the command ctxpvd.exe -s reset). To work around this issue, restart the desktop as prompted. This is a once-only reset that is not required when you log on again. [#340186]
- If you install .NET 4.5 on a personal vDisk and a later image update installs or modifies .NET 4.0, applications that are dependent on .NET 4.5 fail. To work around this issue, distribute .NET 4.5 from the base image as an image update."
- See also the
  — Known Issues
  documentation for the XenApp and XenDesktop 7.6 release.

About Personal vDisk 7.1.3

Known issues from 7.1.1 fixed in version 7.1.3:

- Direct upgrades from personal vDisk 5.6.0 to personal vDisk 7.x may cause the personal vDisk to fail. [#432992]
- Users might only be able to connect intermittently to virtual desktops with personal vDisks. [#437203]
- If a personal vDisk image update operation is interrupted while personal vDisk 5.6.5 or later is upgraded to personal vDisk 7.0 or later, subsequent update operations can fail. [#436145]

About Personal vDisk 7.1.1

Known issues from 7.1 fixed in version 7.1.1:

- Upgrading to Symantec Endpoint Protection 12.1.3 through an image update causes symhelp.exe to report corrupt antivirus definitions. [#423429]
- Personal vDisk can cause pooled desktops to restart if Service Control Manager (services.exe) crashes. [#0365351]

New known issues in version 7.1.1: none

About Personal vDisk 7.1

New in version 7.1:

- You can now use Personal vDisk with desktops running Windows 8.1, and event logging has been improved.
- Copy-on-Write (CoW) is no longer supported in this release. When upgrading from Version 7.0 to 7.1 of Personal vDisk, all changes to data managed by CoW are lost. This was an experimental feature in XenDesktop 7 and was disabled by default, so if you did not enable it, you are not affected.

Known issues from 7.0.1 fixed in version 7.1:

- If the value of the Personal vDisk registry key EnableProfileRedirection is set to 1 or ON, and later, while updating the image, you change it to 0 or OFF, the entire Personal vDisk space might get allocated to user-installed applications, leaving no space for user profiles, which remain on the vDisk. If this profile redirection is disabled for a catalog and you enable it during an image update, users might not be able to log on to their virtual desktop. [#381921]
- The Desktop Service does not log the correct error in the Event Viewer when a Personal vDisk inventory update fails.

[#383331]

- When upgrading to Personal vDisk 7.x, modified rules are not preserved. This issue has been fixed for upgrades from Version 7.0 to Version 7.1. When upgrading from Version 5.6.5 to Version 7.1, you must first save the rule file and then apply the rules again after the upgrade. [#388664]
- Personal vDisks running Windows 8 cannot install applications from the Windows Store. An error message stating, "Your purchase couldn't be completed," appears. Enabling the Windows Update Service does not resolve this issue, which has now been fixed. However, user-installed applications must be reinstalled after the system restarts. [#361513]
- Some symbolic links are missing in Windows 7 pooled desktops with personal vDisks. As a result, applications that store icons in C:\Users\All Users do not display these icons in the Start menu. [#418710]
- A personal vDisk does not start if an Update Sequence Number (USN) journal overflow occurs due to a large number of changes made to the system after an inventory update. [#369846]
- A personal vDisk does not start with status code 0x20 and error code 0x20000028. [#393627]
- Symantec Endpoint Protection 12.1.3 displays the message "Proactive Threat Protection is malfunctioning" and this component's Live Update Status is not available. [#390204]

New known issues in version 7.1: See the
— Known Issues
documentation for the XenDesktop 7.1 release.

About Personal vDisk 7.0.1

New in version 7.0.1: Personal vDisk is now more robust to environment changes. Virtual desktops with personal vDisks now register with the Delivery Controller even if image updates fail, and unsafe system shutdowns no longer put the vDisks into a permanently disabled state. In addition, using rules files you can now exclude files and folders from the vDisks during a deployment.

Known issues from 5.6.13 fixed in version 7.0.1:

- Changes to a group's membership made by users on a pooled virtual desktop might be lost after an image update. [#286227]
- Image updates might fail with a low disk space error even if the personal vDisk has enough space. [#325125]
- Some applications fail to install on virtual desktops with a personal vDisk, and a message is displayed that a restart is required. This is due to a pending rename operation. [#351520]
- Symbolic links created inside the master image do not work on virtual desktops with personal vDisks. [#352585]
- In environments that use Citrix Profile management and personal vDisk, applications that examine user profiles on a system volume might not function properly if profile redirection is enabled. [#353661]
- The inventory update process fails on master images when the inventory is bigger than 2GB. [#359768]
- Image updates fail with error code 112 and personal vDisks are corrupted even if the vDisks have enough free space for the update. [#363003]
- The resizing script fails for catalogs with more than 250 desktops. [#363365]
- Changes made by users to an environment variable are lost when an image update is performed. [#372295]
- Local users created on a virtual desktop with a personal vDisk are lost when an image update is performed. [#377964]
- A personal vDisk may fail to start if an Update Sequence Number (USN) journal overflow occurred due to a large number of changes made to the system after an inventory update. To avoid this, increase the USN journal size to a minimum of 32 MB in the master image and perform an image update. [#369846]
- An issue has been identified with Personal vDisk that prevents the correct functioning of AppSense Environment Manager registry hiving actions when AppSense is used in Replace Mode. Citrix and AppSense are working together to resolve the issue, which is related to the behavior of the RegRestoreKey API when Personal vDisk is installed.[#0353936]

Release-independent known issues

- When an application installed on a personal vDisk (PvD) is related to another application of the same version that is installed on the master image, the application on the PvD could stop working after an image update. This occurs if you uninstall the application from the master image or upgrade it to a later version, because that action removes the files needed by the application on the PvD from the master image. To prevent this, keep the application containing the files needed by the application on the PvD on the master image.
  For example, the master image contains Office 2007, and a user installs Visio 2007 on the PvD; the Office applications and Visio work correctly. Later, the administrator replaces Office 2007 with Office 2010 on the master image, and then updates all affected machines with the updated image. Visio 2007 no longer works. To avoid this, keep Office 2007 in the master image. [#320915]

- When deploying McAfee Virus Scan Enterprise (VSE), use version 8.8 Patch 4 or later on a master image if you use personal vDisk. [#303472]
- If a shortcut created to a file in the master image stops working (because the shortcut target is renamed within PvD), recreate the shortcut. [#367602]
- Do not use absolute/hard links in a master image. [#368678]
- The Windows 7 backup and restore feature is not supported on the personal vDisk. [#360582]
- After an updated master image is applied, the local user and group console becomes inaccessible or shows inconsistent data. To resolve the issue, reset the user accounts on the VM, which requires resetting the security hive. This issue was fixed in the 7.1.2 release (and works for VMs created in later releases), but the fix does not work for VMs that were created with an earlier version and then upgraded. [#488044]
- When using a pooled VM in an ESX hypervisor environment, users see a restart prompt if the selected SCSI controller type is “VMware Paravirtual.” For a workaround, use an LSI SCSI controller type. [#394039]
- After a PvD reset on a desktop created through Provisioning Services, users may receive a restart prompt after logging on to the VM. As a workaround, restart the desktop. [#340186]
- Windows 8.1 desktop users might be unable to log on to their PvD. An administrator might see message "PvD was disabled due to unsafe shutdown" and the PvDActivation log might contain the message "Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]." This occurs when a user’s VM shuts down unsafely. As a workaround, reset the personal vDisk. [#474071]

Install and upgrade

Aug 02, 2016

Personal vDisk 7.x is supported on XenDesktop version 5.6 through the current version. The "System requirements" documentation for each XenDesktop version lists the supported operating systems for Virtual Delivery Agents (VDAs), and the supported versions of hosts (virtualization resources), and Provisioning Services. For details about Provisioning Services tasks, see the Provisioning Services documentation.

Install and enable PvD

PvD is installed automatically when you install or upgrade a VDA for Desktop OS on a machine. If you update the PvD software after installing the VDA, use the PvD MSI provided here (Citrix account credentials required).

Enabling PvD:

- If you are using Machine Creation Services (MCS), PvD is enabled automatically when you create a machine catalog of desktop OS machines that will use a personal vDisk.
- If you are using Provisioning Services (PVS), PvD is enabled automatically when you run the inventory during the master (base) image creation process, or when auto-update runs the inventory for you.

VDA installation offers options to enable PvD (by selecting the “Personal vDisk” checkbox in the graphical interface or by specifying the /baseimage option in the command line interface). However, omitting this action during the VDA install (which is the default) still allows you to use the same image to create both PvD desktops and non-PvD desktops, because PvD is enabled during the catalog creation process.

Add personal vDisks

You add personal vDisks to hosts when you configure a Site. You can choose to use the same storage on the host for VMs and personal vDisks, or you can use different storage for personal vDisks.

Later, you can also add personal vDisks and their storage to existing hosts (connections), but not machine catalogs.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select Add Personal vDisk storage in the Actions pane, and specify the storage location.

Upgrade PvD

The easiest way to upgrade personal vDisk from an earlier 7.x version is to simply upgrade your desktop OS VDAs to the version provided with the most recent XenDesktop version. Then, run the PvD inventory.

You can also upgrade just PvD using the PvD MSI from here.

Uninstall PvD

You can use one of two ways to remove the PvD software:

- Uninstall the VDA; this removes the PvD software as well.
- If you updated PvD using the PvD MSI, then you can uninstall it from the Programs list.

If you uninstall PvD and then want to reinstall the same or a newer version, first back up the registry key HKLM\Software\Citrix\personal vDisk\config, which contains environment configuration settings that might have changed. Then, after installing PvD, reset the registry values that might have changed, by comparing them with the backed-up version.

Configuration and management

Nov 12, 2014

This topic covers items you should consider when configuring and managing a personal vDisk (PvD) environment. It also covers best practice guidelines and task descriptions.

For procedures that include working in the Windows registry:
Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Considerations: personal vDisk size

The following factors affect the size of the main personal vDisk volume:

- **Size of the applications that users will install on their PvDs**
  At restarts, PvD determines the free space remaining in the application area (UserData.v2.vhd). If this falls below 10%, the application area is expanded into any unused profile area space (by default, the space available on the P: drive). The space added to the application area is approximately 50% of the combined free space remaining in both the application area and the profile area.

  For example, if the application area on a 10 GB PvD (which by default is 5 GB) reaches 4.7 GB and the profile area has 3 GB free, the increased space that is added to the application area is calculated as follows:

  increased space = (5.0-4.7)/2 + 3.0/2 = 1.65 GB

  The space added to the application area is only approximate because a small allowance is made for storing logs and for overhead. The calculation and the possible resizing is performed on each restart.

- **Size of users' profiles (if a separate profile management solution is not used)**
  In addition to the space required for applications, ensure there is sufficient space available on personal vDisks to store users' profiles. Include any non-redirected special folders (such as My Documents and My Music) when calculating space requirements. Existing profile sizes are available from the Control Panel (sysdm.cpl).

  Some profile redirection solutions store stub files (sentinel files) instead of real profile data. These profile solutions might appear to store no data initially but actually consume one file directory entry in the file system per stub file; generally, approximately 4 KB per file. If you use such a solution, estimate the size based on the real profile data, not the stub files.

  Enterprise file sharing applications (such as ShareFile and Dropbox) might synchronize or download data to users' profile areas on the personal vDisks. If you use such applications, include enough space in your sizing estimates for this data.

- **Overhead consumed by the template VHD containing the PvD inventory**
  The template VHD contains the PvD inventory data (sentinel files corresponding to the master image content). The PvD application area is created from this VHD. Because each sentinel file or folder comprises a file directory entry in the file system, the template VHD content consumes PvD application space even before any applications are installed by the end user. You can determine the template VHD size by browsing the master image after an inventory is taken. Alternatively, use the following equation for an approximately calculation:

  template VHD size = (number of files on base image) x 4 KB

  Determine the number of files and folders by right-clicking the C: drive on the base VM image and selecting Properties.

For example, an image with 250,000 files results in a template VHD of approximately 1,024,000,000 bytes (just under 1 GB). This space will be unavailable for application installations in the PvD application area.

- **Overhead for PvD image update operations**
  During PvD image update operations, enough space must be available at the root of the PvD (by default, P:) to merge the changes from the two image versions and the changes the user has made to their PvD. Typically, PVD reserves a few hundred megabytes for this purpose, but extra data that was written to the P: drive might consume this reserved space, leaving insufficient for the image update to complete successfully. The PvD pool statistics script (located on the XenDesktop installation media in the Support/Tools/Scripts folder) or the PvD Image Update Monitoring Tool (in the Support/Tools/Scripts\PvdTool folder) can help identify any PvD disks in a catalog that are undergoing an update and that are nearly full.

  The presence of antivirus products can affect how long it takes to run the inventory or perform an update. Performance can improve if you add CtxPvD.exe and CtxPvDSvc.exe to the exclusion list of your antivirus product. These files are located in C:\Program Files\Citrix\personal vDisk\bin. Excluding these executables from scanning by the antivirus software can improve inventory and image update performance by up to a factor of ten.

- **Overhead for unexpected growth (unexpected application installations, and so on)**
  Consider allowing extra (either a fixed amount or a percentage of the vDisk size) to the total size to accommodate unexpected application installations that the user performs during deployment.

How-to: Configure the personal vDisk size and allocation

You can manually adjust the automatic resizing algorithm that determines the size of the VHD relative to the P: drive, by setting the initial size of the VHD. This can be useful if, for example, you know users will install a number of applications that are too big to fit on the VHD even after it is resized by the algorithm. In this case, you can increase the initial size of the application space to accommodate the user-installed applications.

Preferably, adjust the initial size of the VHD on a master image. Alternatively, you can adjust the size of the VHD on a virtual desktop when a user does not have sufficient space to install an application. However, you must repeat that operation on each affected virtual desktop; you cannot adjust the VHD initial size in a catalog that is already created.

Ensure the VHD is big enough to store antivirus definition files, which are typically large.

Locate and set the following registry keys in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config. (Do not modify other settings in this registry key.) All settings must be specified on the master image (except for MinimumVHDSizeInMB, which can be changed on an individual machine); settings specified on the master image are applied during the next image update.

- **MinimumVHDSizeMB**
  Specifies the minimum size (in megabytes) of the application part (C:) of the personal vDisk. The new size must be greater than the existing size but less than the size of the disk minus PvDReservedSpaceMB.

  Increasing this value allocates free space from the profile part on the vDisk to C:. This setting is ignored if a lower value than the current size of the C: drive is used, or if EnableDynamicResizeOfAppContainer is set to 0.

  Default = 2048

- **EnableDynamicResizeOfAppContainer**
  Enables or disables the dynamic resizing algorithm.
  - When set to 1, the application space (on C:) is resized automatically when the free space on C: falls below 10%. Allowed values are 1 and 0. A restart is required to effect the resize.

- When set to 0, the VHD size is determined according to the method used in XenDesktop versions earlier than 7.x

Default = 1

- **EnableUserProfileRedirection**

  Enables or disables redirecting the user's profile to the vDisk.
  - When set to 1, PvD redirects users' profiles to the personal vDisk drive (P: by default). Profiles are generally redirected to P:\Users, corresponding to a standard Windows profile. This redirection preserves the profiles in case the PvD desktop must be reset.
  - When set to 0, all of the space on the vDisk minus PvDReservedSpaceMB is allocated to C:, the application part of the vDisk, and the vDisk drive (P:) is hidden in Windows Explorer. Citrix recommends disabling redirection by setting the value to 0, when using Citrix Profile management or another roaming profile solution.
    This setting retains the profiles in C:\Users instead of redirecting them to the vDisk, and lets the roaming profile solution handle the profiles.

    This value ensures that all of the space on P: is allocated to applications.

    It is assumed that if this value is set to 0, a profile management solution is in place. Disabling profile redirection without a roaming profile solution in place is not recommended because subsequent PvD reset operations result in the profiles being deleted.

  Do not change this setting when the image is updated because it does not change the location of existing profiles, but it will allocate all the space on the Personal vDisk to C: and hide the PvD.

  Configure this value before deploying a catalog. You cannot change it after the catalog is deployed.

  Important: Beginning with XenDesktop 7.1, changes to this value are not honored when you perform an image update. Set the key's value when you first create the catalogs from which the profiles will originate. You cannot modify the redirection behavior later.
  Default = 1

- **PercentOfPvDForApps**

  Sets the split between the application part (C:) and the profile part of the vDisk. This value is used when creating new VMs, and during image updates when EnableDynamicResizeOfAppContainer is set to 0.

  Changing PercentOfPvDForApps makes a difference only when EnableDynamicResizeOfAppContainer is set to 0. By default, EnableDynamicResizeOfAppContainer is set to 1 (enabled), which means is that the AppContainer (which you see as the C drive) only expands when it is close to being full (that is, dynamic) - when less than 10% free space remains.

  Increasing PercentOfPvDForApps only increases the maximum space for which the Apps portion is allowed to expand. It does not provision that space for you immediately. You must also configure the split allocation in the master image, where it will be applied during the next image update.

  If you have already generated a catalog of machines with EnableDynamicResizeOfAppContainer set to 1, then change that setting to 0 in the master image for the next update, and configure an appropriate allocation split. The requested split size will be honored as long as it is larger than the current allocated size for the C drive.

  If you want to maintain complete control over the space split, set this value to 0. This allows full control over the C drive size, and does not rely on a user consuming space below the threshold to expand the drive.

  Default = 50% (allocates equal space to both parts)

- **PvDReservedSpaceMB**
  Specifies the size of the reserved space (in megabytes) on the vDisk for storing Personal vDisk logs and other data.

  If your deployment includes XenApp 6.5 (or an earlier version) and uses application streaming, increase this value by the size of the Rade Cache.

  Default = 512

- **PvDResetUserGroup**
  Valid only for XenDesktop 5.6 - Allows the specified group of users to reset a Personal vDisk. Later XenDesktop releases use Delegated Administration for this.

Other settings:
- **Windows Update Service** - Ensure that you set Windows updates to Never Check for Update and the Windows update service to Disabled in the master image. In the event Windows Update Service needs to run on the PvD, setting it to Never Check for Update helps prevent the updates from being installed on the associated machines.
  Windows 8 Store needs this service to run to install any Modern-style application.

- **Windows updates** - These include Internet Explorer updates and must be applied on the master image.
- **Updates requiring restarts** - Windows updates applied to the master image might require multiple restarts to fully install, depending on the type of patches delivered in those updates. Ensure you restart the master image properly to fully complete the installation of any Windows updates applied to it before taking the PvD inventory.
- **Application updates** - Update applications installed on the master image to conserve space on users' vDisks. This also avoids the duplicate effort of updating the applications on each user's vDisk.

Considerations: Applications on the master image

Some software might conflict with the way that PvD composites the user's environment, so you must install it on the master image (rather than on the individual machine) to avoid these conflicts. In addition, although some other software might not conflict with the operation of PvD, Citrix recommends installing it on the master image.

Applications that must be installed on the master image:
- Agents and clients (for example, System Center Configuration Manager Agent, App-V client, Citrix Receiver)
- Applications that install or modify early-boot drivers
- Applications that install printer or scanner software or drivers
- Applications that modify the Windows network stack
- VM tools such as VMware Tools and XenServer Tools

Applications that should be installed on the master image:
- Applications that are distributed to a large number of users. In each case, turn off application updates before deployment:
  - Enterprise applications using volume licensing, such as Microsoft Office, Microsoft SQL Server
  - Common applications, such as Adobe Reader, Firefox, and Chrome
- Large applications such as SQL Server, Visual Studio, and application frameworks such as .NET

The following recommendations and restrictions apply to applications installed by users on machines with personal vDisks. Some of these cannot be enforced if users have administrative privileges:
- Users should not uninstall an application from the master image and reinstall the same application on their personal vDisk.
- Take care when updating or uninstalling applications on the master image. After you install a version of an application on

the image, a user might install an add-on application (for example, a plug-in) that requires this version. If such a dependency exists, updating or uninstalling the application on the image might make the add-on malfunction. For example, with Microsoft Office 2010 installed on a master image, a user installs Visio 2010 on their personal vDisk. A later upgrade of Office on the master image might make the locally-installed Visio unusable.
- Software with hardware-dependent licenses (either through a dongle or signature-based hardware) is unsupported.

Considerations: Provisioning Services

When using Provisioning Services with PvD:
- The Soap Service account must be added to the Administrator node of Studio and must have the Machine Administrator or higher role. This ensures that the PvD desktops are put into the Preparing state when the Provisioning Services (PVS) vDisk is promoted to production.
- The Provisioning Service versioning feature must be used to update the personal vDisk. When the version is promoted to production, the Soap Service puts the PvD desktops into the Preparing state.
- The personal vDisk size should always be larger than the Provisioning Services write cache disk (otherwise, Provisioning Services might erroneously select the personal vDisk for use as its write cache).
- After you create a Delivery Group, you can monitor the personal vDisk using the PvD Image Update Monitoring Tool or the Resize and poolstats scripts (personal-vdisk-poolstats.ps1).

Size the write cache disk correctly. During normal operation, PvD captures most user writes (changes) and redirects them to the personal vDisk. This implies that you can reduce the size of the Provisioning Services write cache disk. However, when PvD is not active (such as during image update operations), a small Provisioning Services write cache disk can fill up, resulting in machine crashes.

Citrix recommends that you size Provisioning Services write cache disks according to Provisioning Services best practice and add space equal to twice the size of the template VHD on the master image (to accommodate merge requirements). It is extremely unlikely that a merge operation will require all of this space, but it is possible.

When using Provisioning Services to deploy a catalog with PvD-enabled machines:
- Follow the guidance in the Provisioning Services documentation.
- You can change the power action throttling settings by editing the connection in Studio; see below.
- If you update the Provisioning Services vDisk, after you install/update applications and other software and restart the vDisk, run the PvD inventory and then shut down the VM. Then, promote the new version to Production. The PvD desktops in the catalog should automatically enter the Preparing state. If they do not, check that the Soap Service account has machine administrator or higher privileges on the Controller.

The Provisioning Services test mode feature enables you to create a test catalog containing machines using an updated master image. If tests confirm the test catalog's viability, you can promote it to production.

Considerations: Machine Creation Services

When using Machine Creation Services (MCS) to deploy a catalog with PvD-enabled machines:
- Follow the guidance in the XenDesktop documentation.
- Run a PvD inventory after you create the master image and then power off the VM (PvD will not function correctly if you do not power off the VM). Then, take a snapshot of the master image.
- In the Create Machine Catalog wizard, specify the personal vDisk size and drive letter.
- After you create a Delivery Group, you can monitor the personal vDisk using the PvD Image Update Monitoring Tool or the Resize and poolstats scripts (personal-vdisk-poolstats.ps1).
- You can change the power action throttling settings by editing the connection in Studio; see below.

- If you update the master image, run the PvD inventory after you update the applications and other software on the image, and then power off the VM. Then, take a snapshot of the master image.
- Use the PvD Image Update Monitoring Tool or the personal-vdisk-poolstats.ps1 script to validate that there is sufficient space on each PvD-enabled VM that will use the updated master image.
- After you update the machine catalog, the PvD desktops enter the Preparing state as they individually process the changes in the new master image. The desktops are updated according to the rollout strategy specified during the machine update.
- Use the PvD Image Update Monitoring Tool or the personal-vdisk-poolstats.ps1 script to monitor the PvD in the Preparing state.

How-to: Exclude files and folders from vDisks

Use the rules files to exclude files and folders from the vDisks. You can do this when the personal vDisks are in deployment. The rules files are named custom_*_rules.template.txt and are located in the \config folder. Comments in each file provide additional documentation.

How-to: Run the inventory when updating a master image

When you enable PvD and after any update to the master image after installation, it is important to refresh the disk's inventory (called "run the inventory") and create a new snapshot.

Because administrators, not users, manage master images, if you install an application that places binary files in the administrator's user profile, the application is not available to users of shared virtual desktops (including those based on pooled machine catalogs and pooled with PvD machine catalogs). Users must install such applications themselves.

It is best practice to take a snapshot of the image after each step in this procedure.

1. Update the master image by installing any applications or operating system updates, and performing any system configuration on the machine.
   For master images based on Windows XP that you plan to deploy with Personal vDisks, check that no dialog boxes are open (for example, messages confirming software installations or prompts to use unsigned drivers). Open dialog boxes on master images in this environment prevent the VDA from registering with the Delivery Controller. You can prevent prompts for unsigned drivers using the Control Panel. For example, navigate to System > Hardware > Driver Signing, and select the option to ignore warnings.
2. Shut down the machine. For Windows 7 machines, click Cancel when Citrix Personal vDisk blocks the shutdown.
3. In the Citrix Personal vDisk dialog box, click Update Inventory. This step may take several minutes to complete.
   Important: If you interrupt the following shutdown (even to make a minor update to the image), the Personal vDisk's inventory no longer matches the master image. This causes the Personal vDisk feature to stop working. If you interrupt the shutdown, you must restart the machine, shut it down, and when prompted click Update Inventory again.
4. When the inventory operation shuts down the machine, take a snapshot of the master image.

You can export an inventory to a network share and then import that inventory to a master image. For details, see Export and import a PvD inventory.

How-to: Configure connection throttling settings

The Citrix Broker Service controls the power state of the machines that provide desktops and applications. The Broker Service can control several hypervisors through a Delivery Controller. Broker power actions control the interaction between a Controller and the hypervisor. To avoid overloading the hypervisor, actions that change a machine's power state are assigned a priority and sent to the hypervisor using a throttling mechanism. The following settings affect the throttling. You

specify these values by editing a connection (Advanced page) in Studio.

To configure connection throttling values:

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Edit Connection in the Actions pane.
3. You can change the following values:
   - **Simultaneous actions (all types)** - The maximum number of simultaneous in-progress power actions allowed. This setting is specified as both an absolute value and as a percentage of the connection to the hypervisor. The lower of the two values is used.
     Default = 100 absolute, 20%
   - **Simultaneous Personal vDisk inventory updates** - The maximum number of simultaneous Personal vDisk power actions allowed. This setting is specified as both an absolute value and a percentage of the connection. The lower of the two values is used.
     Default = 50 absolute, 25%

     To calculate the absolute value: determine the total IOPS (TIOPS) supported by the end-user storage (this should be specified by the manufacturer or calculated). Using 350 IOPS per VM (IOPS/VM), determine the number of VMs that should be active at any given time on the storage. Calculate this value by dividing total IOPS by IOPS/VM.

     For example, if the end-user storage is 14000 IPS, the number of active VMs is 14000 IOPS / 350 IOPS/VM = 40.
   - **Maximum new actions per minute** - The maximum number of new power actions that can be sent to the hypervisor per minute. Specified as an absolute value.
     Default = 10

To help identify optimal values for these settings in your deployment:

1. Using the default values, measure the total response time for an image update of a test catalog. This is the difference between the start of an image update (T1) and when the VDA on the last machine in the catalog registers with the Controller (T2). Total response time = T2 - T1.
2. Measure the input/output operations per second (IOPS) of the hypervisor storage during the image update. This data can serve as a benchmark for optimization. (The default values may be the best setting; alternatively, the system might max out of IOPS, which will require lowering the setting values.)
3. Change the “Simultaneous Personal vDisk inventory updates” value as described below (keeping all other settings unchanged).
   1. Increase the value by 10 and measure the total response time after each change. Continue to increase the value by 10 and test the result, until deterioration or no change in the total response time occurs.
   2. If the previous step resulted in no improvement by increasing the value, decrease the value in increments of 10 and measure the total response time after each decrease. Repeat this process until the total response time remains unchanged or does not improve further. This is likely the optimal PvD power action value.
4. After obtaining the PvD power action setting value, tweak the simultaneous actions (all types) and maximum new actions per minute values, one at a time. Follow the procedure described above (increasing or decreasing in increments) to test different values.

How-to: System Center Configuration Manager 2007 with PvD

System Center Configuration Manager (Configuration Manager) 2012 requires no special configuration and can be installed in the same way as any other master image application. The following information applies only to System Center Configuration Manager 2007. Configuration Manager versions earlier than Configuration Manager 2007 are not supported.

Complete the following to use Configuration Manager 2007 agent software in a PvD environment.

1. Install the Client Agent on the master image.
    1. Install the Configuration Manager client on the master image.
    2. Stop the ccmexec service (SMS Agent) and disable it.
    3. Delete SMS or client certificates from the local computer certificate store as follows:
        - Mixed mode: Certificates (Local Computer)\SMS\Certificates
        - Native mode
            - Certificates (Local Computer)\Personal\Certificates
            - Delete the client certificate that was issued by your certificate authority (usually, an internal Public Key Infrastructure)
    4. Delete or rename C:\Windows\smscfg.ini.
2. Remove information that uniquely identifies the client.
    1. (Optional) Delete or move log files from C:\Windows\System32\CCM\Logs.
    2. Install the Virtual Delivery Agent (if not installed previously), and take the PvD inventory.
    3. Shut down the master image, take a snapshot, and create a machine catalog using this snapshot.
3. Validate personal vDisk and start services. Complete these steps once on each PvD desktop, after it has been started for the first time. This can be done using a domain GPO, for example.
    - Confirm that PvD is active by checking for the presence of the registry key HKLM\Software\Citrix\personal vDisk\config\virtual.
    - Set the ccmexec service (SMS agent) to Automatic and start the service. The Configuration Manager client contacts the Configuration Manager server, and retrieves new unique certificates and GUIDs.

Tools

May 01, 2015

You can use the following tools and utilities to tailor, expedite, and monitor PvD operations.

Custom rules files

The custom rule files provided with PvD let you modify the default behavior of PvD image updates in the following ways:

- The visibility of files on the PvD
- How changes made to the files are merged
- Whether the files are writable

For detailed instructions on the custom rules files and the CoW feature, refer to the comments in the files located in C:\ProgramData\Citrix\personal vDisk\Config on the machine where PvD is installed. The files named "custom_*" describe the rules and how to enable them.

Resize and poolstats scripts

Two scripts are provided to monitor and manage the size of PvDs; they are located in the Support\Tools\Scripts folder on the XenDesktop installation media. You can also use the PvD Image Update Monitoring Tool, which is located in the Support\Tools\Scripts\PvdTool folder; see http://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/ for details.

Use resize-personalvdisk-pool.ps1 to increase the size of the PvDs in all of the desktops in a catalog. The following snap-ins or modules for your hypervisor must be installed on the machine running Studio:

- XenServer requires XenServerPSSnapin
- vCenter requires vSphere PowerCli
- System Center Virtual Machine Manager requires the VMM console

Use personal-vdisk-poolstats.ps1 to check the status of image updates and to check the space for applications and user profiles in a group of PvDs. Run this script before updating an image to check whether any desktop is running out of space, which helps prevent failures during the update. The script requires that Windows Management Instrumentation (WMI-In) firewall is enabled on the PvD desktops. You can enable it on the master image or through GPO.

If an image update fails, the entry in the Update column gives the reason.

Reset the application area

If a desktop becomes damaged or corrupted (by installing a broken application or some other cause), you can revert the application area of the PvD to a factory-default (empty) state. The reset operation leaves user profile data intact.

To reset the application area of the PvD, use one of the following methods:

- Log on to the user's desktop as Administrator. Launch a command prompt, and run the command C:\Program Files\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset.
- Locate the user's desktop in Citrix Director. Click Reset Personal vDisk and then click OK.

Export and import a PvD inventory

The image update process is an integral part of rolling out new images to PvD desktops; it includes adjusting the existing Personal vDisk to work with the new base image. For deployments that use Machine Creations Services (MCS), you can

export an inventory from an active VM to a network share, and then import it into a master image. A differential is calculated using this inventory in the master image. Although using the export/import inventory feature is not mandatory, it can improve the performance of the overall image update process.

To use the export/import inventory feature, you must be an administrator. If required, authenticate to the file share used for the export/import with "net use." The user context must be able to access any file shares used for the export/import.

- To export an inventory, run the export command as an administrator on a machine containing a VDA with PvD enabled (minimum version 7.6):
  Ctxpvdsvc.exe exportinventory "<path-to-export-location>"

  The software detects the current inventory's location and exports the inventory to a folder named "ExportedPvdInventory" to the specified location. Here's an excerpt from the command output:
  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe exportinventory
  \\share location\ExportedInventory
  Current inventory source location C:\CitrixPvD\Settings\Inventory\VER-LAS
  ...
  Exporting current inventory to location \\ ....
  ...
  Deleting any pre-existing inventory folder at \\ ....
  .Successfully exported current inventory to location \\ .... Error code = OPS
- To import a previously-exported inventory, run the import command as an administrator on the master image:

To import

Run the import command as an administrator on the master image.

Ctxpvdsvc.exe importinventory "<path-to-exported-inventory>"

The <path to exported inventory> should be the full path to the inventory files, which is usually <network location\ExportedPvdInventory>.

The inventory is obtained from the import location (where it was previously exported using the exportinventory option) and imports the inventory to the inventory store on the master image. Here's an excerpt of the command output:
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe importinventory
\\share location\ExportedInventory\ExportedPvdInventory
Importing inventory \\share location\ExportedInventory\ExportedPvdInventory
...
Successfully added inventory \\share location\ExportedInventory\ExportedPvdInventory to the store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
After the export, the network share should include the following filenames. After the import, the inventory store on the master image should include the same file names.

- Components.DAT
- files_rules
- folders_rules
- regkey_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT

- SNAPSHOT.DAT
- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

Back up and restore

Important: The scripts do not move PvDs to the new storage location. You must perform that operation in some other way.
Two PowerShell scripts supplied on the product installation media (in the Support\Tools\Scripts folder) allow you to back up and restore Personal vDisks. Use the backup and restore scripts to migrate existing PvDs and user associations from one catalog to another. This can be useful if you are changing your PvD storage. The backup script creates an .xml file with metadata from an existing catalog. The metadata contains the current location of the PvDs on the storage, and the user associations with the PvDs. The restore script uses the .xml file to associate the PvDs with a new catalog and assign the correct users to them.

- migration-backup.ps1 captures the mapping between each user and their Personal vDisk in a machine catalog and stores this information in an .xml file
- migration-restore.ps1 uses the .xml file to re-create a user's desktop in a machine catalog

Before backing up and restoring, note the following:

- The scripts work with the hypervisor API so the hypervisor's PowerShell snap-in must be installed on the Controller where the scripts are executed
- Run the scripts from a location that has access to the Controller where the machine catalog was created
- The scripts are supported on the following hypervisor platforms: Citrix XenServer, Microsoft Hyper-V, and VMware ESX

Back up a machine catalog

Perform a backup when a change is made to a machine catalog. You can perform a backup while the machines in the catalog are active.

Use migration-backup.ps1 to back up any machine catalog containing Personal vDisks. The script asks for the name of the machine catalog and connection information for the hypervisor. It then iterates through all of the user-assigned machines in the machine catalog and, for each machine, stores the mapping between the Personal vDisk storage and the assigned user. This information is located in an .xml file, which has the following structure:

```
<PVDMigration>
 <hypervisor>
  <type></type>
 </hypervisor>
 <PVD>
  <DiskId></DiskId>
  <DiskName></DiskName>
  <SRName></SRName>
  <SRID></SRID>
  <UserName></UserName>
  <UserSid></UserSid>
  <State></State>
 </PVD>
</PVDMigration>
```

- PvDMigration.hypervisor.Type supports VMware ESX, Citrix XenServer, and Microsoft Hyper-V.

- PvDMigration.PVD stores information on where the Personal vDisk is stored and the user associated with it.
- PvDMigration.PVD.DiskId is the unique identifier of the vDisk on the hypervisor on which the backup was taken.
- PvDMigration.PVD.DiskName is the name of the .vhd or .vmdk file.
- PvDMigration.PVD.SRName is the name of the storage provider when the backup was taken.
- PvDMigration.PVD.SRID is the unique identifier of the storage provider on the hypervisor on which the backup was taken.
- PvDMigration.PVD.UserName is the name of the user associated with this vDisk.
- PvDMigration.PVD.UserSid is the SID of the user associated with this vDisk.
- PvDMigration.PVD.State indicates the state of this vDisk. This can be either "backed up" or "processed." It is "backed up" after the initial backup; the state changes to "processed" after the .xml file is used for restoring from the backup.

Restore a machine catalog

Before restoring, note the following:
- You can only restore a machine catalog that shares the same master image as that of the backed-up machine catalog
- You must create a new master image by updating the inventory of the master image that the backed-up machine catalog was created from

Use migration-restore.ps1 to restore any machine catalog containing Personal vDisks. The script takes the following inputs:
- The .xml file created during the backup process
- The name of the machine catalog to restore
- The name of the location where the unattached Personal vDisks are stored. This is listed in the .xml file
- Hypervisor connection information

The migration-restore.ps1 script finds any unassigned machines in the machine catalog and assigns users to them. It also attaches users' Personal vDisks to the machines.

Example scenario 1: Restore a machine catalog and its Personal vDisks using new machine names

In this scenario, an entire machine catalog and the Personal vDisks attached to the machines in it are restored. The machines are given new names. This scenario might occur when your hypervisor or a storage host has failed, or when you migrate users to a new infrastructure.

1. Run migration-backup.ps1 to capture the user-to-Personal-vDisk mapping in the .xml file.
2. Using a backup solution, move or capture the Personal vDisks from the original machine catalog on to a disk:
   - VMware ESX or Microsoft Hyper-V: Personal vDisks are located on the storage specified by the Controller, in a folder containing the name of the machine to which the vDisk is attached.
   - Citrix XenServer: Personal vDisks are located in the root of the storage specified by the Controller. The name of each vDisk is a GUID.
3. Restore the Personal vDisks from the original machine catalog using a storage backup solution:
   - ESX or Hyper-V: Locate the vDisks in a new folder of the new storage resource. Alternatively, leave the vDisks in the original path on the new storage resource.
   - XenServer: Locate the vDisks in the root of the new storage resource.
4. Create a Provisioning Services vDisk or a Machine Creation Services snapshot from the master image, which you used to create the failed machine catalog.
5. Run Update Inventory from the Start menu on the vDisk or snapshot.
6. Re-create the machine catalog in Studio using a different naming convention as the failed (original) machine catalog. This generates a catalog of new machines, each with a new Personal vDisk, that the site database recognizes.
7. Verify that the re-created machine catalog is assigned to the correct Delivery Group.
8. Verify that the Delivery Group is in maintenance mode and the machines in it are shut down.

9. Edit the .xml file generated by the backup script:
   - ESX or Hyper-V: If you restored the vDisks to a new folder on the new storage resource in Step 3, for every PVD section in the file, replace the folder name in DiskName with the location of the restored vDisks. If you restored the vDisks to the original path on the new storage, skip this step.
   - XenServer: Skip this step.
10. On the Controller, run migration-restore.ps1, specifying the name of the .xml file and the location where the backed-up vDisks are stored.

Example scenario 2: Restore a machine catalog and its Personal vDisks reusing existing machine names

In this scenario, an entire machine catalog and the Personal vDisks attached to the machines in it are restored. Existing (failed) machine names are reused. This scenario might occur when your hypervisor or a storage host has failed.

1. Run migration-backup.ps1 to capture the user-to-Personal-vDisk mapping.
2. Using a backup solution, move or capture the Personal vDisks from the original machine catalog on to a disk:
   - ESX or Hyper-V: Personal vDisks are located on the storage specified by the Controller, in a folder containing the name of the machine to which the vDisk is attached.
   - XenServer: Personal vDisks are located in the root of the storage specified by the Controller. The name of each vDisk is a GUID.
3. Restore the Personal vDisks from the original machine catalog using a storage backup solution:
   - ESX or Hyper-V: Locate the vDisks in a new folder of the new storage resource.
   - XenServer: Locate the vDisks in the root of the new storage resource.
4. Create a Provisioning Services vDisk or a Machine Creation Services snapshot from the master image that you used to create the failed machine catalog.
5. Run Update Inventory from the Start menu on the vDisk or snapshot.
6. Re-create the machine catalog in Studio using the same naming convention as the failed machine catalog. This generates a catalog of new machines, each with a new Personal vDisk, that the site database recognizes.
7. Verify that the re-created machine catalog is assigned to the correct Delivery Group.
8. Verify that the Desktop Group is in maintenance mode and the machines in it are shut down.
9. Edit the .xml file generated by the backup script:
   - ESX or Hyper-V: For every PVD section in the file, replace the folder name in DiskName with the location of the restored vDisks.
   - XenServer: Skip this step.
10. Run the migration-restore.ps1 script on the Controller with the modified .xml file as an input. The script attaches the vDisks without moving them.
11. Verify the users' data has been successfully restored.

Example scenario 3: Restore a subset of Personal vDisks in a machine catalog

In this scenario, some, but not all, of the Personal vDisks in a machine catalog have failed and are restored. The virtual machines in the catalog have not failed.

1. Run migration-backup.ps1 to capture the user-to-Personal-vDisk mapping in the .xml file.
2. The .xml file has a PVD section for each user in the machine catalog. For any users whose Personal vDisks do not need restoring, remove the users and their associated sections from the file.
3. Restore the Personal vDisks from the original machine catalog using a backup solution, as described in the one of the other scenarios:
   - To use new machine names, follow example scenario 1.
   - To preserve machine names, follow example scenario 2.
4. Ensure there are enough unassigned machines in the catalog. Add machines if necessary. You need one new machine for

each user whose vDisk you want to restore.

5. Verify that the Desktop Group is in maintenance mode and the machines in it are shut down.
6. On the Controller, run migration-restore.ps1 with the modified .xml file as an input.
7. Verify the users' data has been successfully restored.

Displays, messages, and troubleshooting

Dec 01, 2014

In Studio, when you choose a PvD-enabled machine in a machine catalog, the "PvD" tab provides monitoring status during image updates, plus estimated completion time and progress. The possible state displays during an image update are: Ready, Preparing, Waiting, Failed, and Requested.

An image update can fail for different reasons, including lack of space or a desktop not finding the PvD in sufficient time. When Studio indicates that an image update failed, an error code with descriptive text is provided to help troubleshooting. Use the Personal vDisk Image Update Monitoring Tool or the personal-vdisk-poolstats.ps1 script to monitor image update progress and obtain error codes associated with the failure.

If an image update fails, the following log files can provide further troubleshooting information:

- PvD service log - C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- PvD activation log i- P:\PVDLOGS\PvDActivation.log.txt

The most recent content is at the end of the log file.

Error messages: 7.6 and later

The following errors are valid for PvD version 7.6 and later:

- **An internal error occurred. Review the Personal vDisk logs for further details. Error code %d (%s)**
  This is a catch-all for uncategorized errors, so it has no numeric value. All unexpected error encountered during inventory creation or Personal vDisk update are indicated by this error code.
  - Collect logs and contact Citrix support.
  - If this error occurs during catalog update, roll back the catalog to the previous version of the gold image.
- **There are syntax errors in the rule files. Review the logs for further details.**
  Error code 2. The rule file contains syntax errors. The Personal vDisk log file contains the name of the rule file and line number where the syntax error was found. Fix the syntax error in the rule file and retry the operation.
- **The inventory stored in the Personal vDisk corresponding to the previous version of the master image is corrupt or unreadable.**
  Error code 3. The last inventory is stored in “UserData.V2.vhd” in “\ProgramData\CitrixPvD\Settings\Inventory\VER-LAST”. Restore the inventory corresponding to the last version of the master image by importing the ‘VER-LAST’ folder from a known working PvD machine associated with the previous version of the master image.
- **The inventory stored in the Personal vDisk corresponding to the previous version of the master image is higher version.**
  Error code 4. This is caused by personal vDisk version incompatibility between the last master image and the current master image. Retry updating the catalog after installing the latest version of personal vDisk in the master image.
- **Change journal overflow was detected.**
  Error code 5. A USN journal overflow was caused by a large number of changes made to the master image while creating the inventory. If this continues to occur after multiple attempts, use procmon to determine if third party software is creating/deleting a large number of files during inventory creation.
- **The Personal vDisk could not find a disk attached to the system for storing user data.**
  Error code 6. First, verify that the PvD disk is attached to the VM through the hypervisor console. This error typically happens due to “Data Leak Prevention” software preventing access to the PvD disk. If the PvD disk is attached to the

VM, try adding an exception for “attached disk” in the “Data Leak Prevention” software configuration.

- **The system has not been rebooted post-installation. Reboot to implement the changes.**
  Error code 7. Restart the desktop and retry the operation.

- **Corrupt installation. Try re-installing Personal vDisk.**
  Error code 8. Install personal vDisk and try again.

- **Personal vDisk inventory is not up to date. Update the inventory in the master image, and then try again.**
  Error code 9. The personal vDisk inventory was not updated in the master image before shutting down the desktop. Restart the master image and shut down the desktop through the “Update personal vDisk” option, and then create a new snapshot; use that snapshot to update the catalog.

- **An internal error occurred while starting the Personal vDisk. Review the Personal vDisk logs for further details.**
  Error code 10. This could be caused by the PvD driver failing to start a virtualization session due to an internal error or personal vDisk corruption. Try restarting the desktop through the Controller. if the problem persists, collect the logs and contact Citrix Support.

- **The Personal vDisk timed out while trying to find a storage disk for users' personalization settings.**
  Error code 11. This error occurs when the PvD driver fails to find the PvD disk within 30 seconds after restart. This is usually caused by an unsupported SCSI controller type or storage latency. If this occurs with all desktops in the catalog, change the SCSI controller type associated with the “Template VM” / “Master VM” to a type supported by personal vDisk technology. If this occurs with only some desktops in the catalog, it might be due to spikes in storage latency due to a large number of desktops starting at the same time. Try limiting the maximum active power actions setting associated with the host connection.

- **The Personal vDisk has been de-activated because an unsafe system shutdown was detected. Restart the machine.**
  Error code 12. This could be due to a desktop failing to complete the boot process with PvD enabled. Try restarting the desktop. If the problem persists, watch the desktop startup through the hypervisor console and check if the desktop is crashing. If a desktop crashes during startup, restore the PvD from backup (if you maintain one) or reset the PvD.

- **The drive letter specified for mounting the Personal vDisk is not available.**
  Error code 13. This could be caused by PvD failing to mount the PvD disk at the mount specified by the administrator. The PvD disk will fail to mount if the drive letter is already used by other hardware. Select a different letter as the mount point for the personal vDisk.

- **Personal vDisk kernel mode drivers failed to install.**
  Error code 14. Personal vDisk installs drivers during the first inventory update after installation. Some antivirus products prevent installation of the driver when attempted outside the context of an installer. Temporarily disable the antivirus real time scan or add exceptions in the antivirus for PvD drivers during the first time inventory creation.

- **Cannot create a snapshot of the system volume. Make sure that the Volume Shadow Copy service is enabled.**
  Error code 15. This could occur because the Volume Shadow Copy service is disabled. Enable the Volume Shadow Copy service and retry taking an inventory.

- **The change journal failed to activate. Try again after waiting for few minutes.**
  Error code 16. Personal vDisk uses change journal for tracking changes made to master image. During an inventory update, if PvD detects that the change journal is disabled, it attempts to enable it; this error occurs when that attempt fails. Wait for few minutes and retry.

- **There is not enough free space in the system volume.**
  Error code 17. There is not enough free space available on the C drive of the desktop for the image update operation. Expand the system volume or removed unused files to free space in the system volume. The image update should begin again after the next restart.

- **There is not enough free space in the Personal vDisk storage. Expand Personal vDisk storage to provide more space.**
  Error code 18. There is not enough free space available on the personal vDisk drive when performing an image update operation. Expand personal vDisk storage or remove unused files to free space in the personal vDisk storage. The image update should restart after next reboot.

- **Personal vDisk storage is over-committed. Expand Personal vDisk storage to provide more space.**
  Error code 19. There is not enough free space available on the personal vDisk drive to fully accommodate thick provisioned “UserData.V2.vhd”. Expand the personal vDisk storage or remove unused files to free space in the personal vDisk storage.

- **Corrupt system registry.**
  Error code 20. The system registry is corrupt, damaged, missing, or unreadable. Reset the personal vDisk or restore it from an earlier backup.

- **An internal error occurred while resetting the Personal vDisk. Check Personal vDisk logs for further details.**
  Error code 21. This is a catch-all for all the errors encountered during a personal vDisk reset. Collect the logs and contact Citrix Support.

- **Failed to reset the Personal vDisk because there is not enough free space in the personal vDisk storage.**
  Error code 22. There is not enough free space available on the Personal vDisk drive when performing a reset operation. Expand the personal vDisk storage or remove unused files to free space in the personal vDisk storage.

Error messages: earlier than 7.6

The following errors are valid for PvD 7.x versions earlier than 7.6:

- **Startup failed. Personal vDisk was unable to find a storage disk for user personalization settings.**
  The PvD software could not find the Personal vDisk (by default, the P: drive) or could not mount it as the mount point selected by the administrator when they created the catalog.
  - Check the PvD service log for following entry: "PvD 1 status --> 18:183".
  - If you are using a version of PvD earlier than Version 5.6.12, upgrading to the latest version resolves this issue.
  - If you are using Version 5.6.12 or later, use the disk management tool (diskmgmt.msc) to determine whether the P: drive is present as an unmounted volume. If present, run chkdsk on the volume to determine if it is corrupt, and try to recover it using chkdsk.
- **Startup failed. Citrix Personal vDisk failed to start. For further assistance .... Status code: 7, Error code: 0x70**
  Status code 7 implies that an error was encountered while trying to update the PvD. The error could be one of the following:

Error code	Description
0x20000001	Failed to save the diff package, most likely due to lack of free disk space inside the VHD.
0x20000004	Failed to acquire required privileges for updating the PvD.

Error code	Description
0x20000006	Failed to load hive from the PvD image or from PvD inventory, most likely due to corrupt PvD image or inventory.
0x20000007	Failed to load the file system inventory, most likely due to a corrupt PvD image or inventory.
0x20000009	Failed to open the file containing file system inventory, most likely due to a corrupt PvD image or inventory.
0x2000000B	Failed to save the diff package, most likely due to lack of free disk space inside the VHD.
0x20000010	Failed to load the diff package.
0x20000011	Missing rule files.
0x20000021	Corrupt PvD inventory.
0x20000027	The catalog "MojoControl.dat" is corrupt.
0x2000002B	Corrupt or missing PvD inventory.
0x2000002F	Failed to register user installed MOF on image update, upgrade to 5.6.12 to fix the issue.
0x20000032	Check the PvDactivation.log.txt for the last log entry with a Win32 error code.
0x20	Failed to mount application container for image update, upgrade to 5.6.12 to fix the issue.
0x70	There is not enough space on the disk.

- **Startup failed. Citrix Personal vDisk failed to start [or Personal vDisk encountered an internal error]. For further assistance ... Status code: 20, Error code 0x20000028**
  The personal vDisk was found but a PvD session could not be created.

  Collect the logs and check SysVol-IvmSupervisor.log for session creation failures:
  1. Check for the following log entry " IvmpNativeSessionCreate: failed to create native session, status XXXXX".
  2. If the status is 0xc00002cf, fix the problem by adding a new version of the master image to the catalog. This status code implies that the USN Journal overflowed due to a large number of changes after an inventory update.
  3. Restart the affected virtual desktop. If the problem persists, contact Citrix Technical Support.
- **Startup failed. Citrix Personal vDisk has been deactivated because an unsafe system shutdown was detected. To retry, select Try again. If the problem continues, contact your system administrator.**
  The pooled VM cannot complete its startup with the PvD enabled. First determine why startup cannot be completed. Possible reasons are that a blue screen appears because:
  - An incompatible antivirus product is present, for example old versions of Trend Micro, in the master image.

- The user has installed software that is incompatible with PvD. This is unlikely, but you can check it by adding a new machine to the catalog and seeing whether it restarts successfully.
- The PvD image is corrupt. This has been observed in Version 5.6.5.

To check if the pooled VM is displaying a blue screen, or is restarting prematurely:

- Log on to the machine through the hypervisor console.
- Click Try Again and wait for the machine to shut down.
- Start the machine through Studio.
- Use the hypervisor console to watch the machine console as it starts.

Other troubleshooting:

- Collect the memory dump from the machine displaying the blue screen, and send it for further analysis to Citrix Technical Support.
- Check for errors in the event logs associated with the PvD:
  1. Mount UserData.V2.vhd from the root of the P: drive using DiskMgmt.msc by clicking Action > Attach VHD.
  2. Launch Eventvwr.msc.
  3. Open the system event log (Windows\System32\winevt\logs\system.evtx) from UserData.V2.vhd by clicking Action > Open saved logs.
  4. Open the application event log (Windows\System32\winevt\logs\application.evtx) from UserData.V2.vhd by clicking Action > Open saved logs.

- **The Personal vDisk cannot start. The Personal vDisk could not start because the inventory has not been updated. Update the inventory in the master image, then try again. Status code: 15, Error code: 0x0**
  The administrator selected an incorrect snapshot while creating or updating the PvD catalog (that is, the master image was not shut down using Update Personal vDisk when creating the snapshot).

Events logged by Personal vDisk

If Personal vDisk is not enabled, you can view the following events in Windows Event Viewer. Select the Applications node in the left pane; the Source of the events in the right pane is Citrix Personal vDisk. If Personal vDisk is enabled, none of these events are displayed.

An Event ID of 1 signifies an information message, an ID of 2 signifies an error. Not all events may be used in every version of Personal vDisk.

Event ID	Description
1	Personal vDisk Status: Update Inventory Started.
1	Personal vDisk Status: Update Inventory completed. GUID: %s.
1	Personal vDisk Status: Image Update Started.
1	Personal vDisk Status: Image Update completed.
1	Reset in progress.
1	OK.

Event ID	Description
2	Personal vDisk Status: Update Inventory Failed with: %s.
2	Personal vDisk Status: Image Update Failed with: %s.
2	Personal vDisk Status: Image Update Failed with Internal Error.
2	Personal vDisk Status: Update Inventory Failed with: Internal Error.
2	Personal vDisk has been disabled because of an improper shutdown.
2	Image update failed. Error code %d.
2	Personal vDisk encountered an internal error. Status code[%d] Error code[0x%X].
2	Personal vDisk reset failed.
2	Unable to find disk for storing user personalization settings.
2	There is not enough space available on the storage disk to create a Personal vDisk container.

User profiles

Sep 25, 2015

By default, Citrix Profile management is installed silently on master images when you install the Virtual Delivery Agent, but you do not have to use Profile management as a profile solution.

To suit your users' varying needs, you can use XenApp and XenDesktop policies to apply different profile behavior to the machines in each Delivery Group. For example, one Delivery Group might require Citrix mandatory profiles, whose template is stored in one network location, while another Delivery Group requires Citrix roaming profiles stored in another location with several redirected folders.

- If other administrators in your organization are responsible for XenApp and XenDesktop policies, work with them to ensure that they set any profile-related policies across your Delivery Groups.
- Profile management policies can also be set in Group Policy, in the Profile management .ini file, and locally on individual virtual machines. These multiple ways of defining profile behavior are read in the following order:
  1. Group Policy (.adm or .admx files)
  2. XenApp and XenDesktop policies in the Policy node
  3. Local policies on the virtual machine that the user connects to
  4. Profile management .ini file

  For example, if you configure the same policy in both Group Policy and the Policy node, the system reads the policy setting in Group Policy and ignores the XenApp and XenDesktop policy setting.

Whichever profile solution you choose, Director administrators can access diagnostic information and troubleshoot user profiles. For more information, see the Director documentation.

If you use the Personal vDisk feature, Citrix user profiles are stored on virtual desktops' Personal vDisks by default. Do not delete the copy of a profile in the user store while a copy remains on the Personal vDisk. Doing so creates a Profile management error, and causes a temporary profile to be used for logons to the virtual desktop.

Automatic configuration

The desktop type is automatically detected, based on the Virtual Delivery Agent installation and, in addition to the configuration choices you make in Studio, sets Profile management defaults accordingly.

The policies that Profile management adjusts are shown in the table below. Any non-default policy settings are preserved and are not overwritten by this feature. Consult the Profile management documentation for information about each policy. The types of machines that create profiles affect the policies that are adjusted. The primary factors are whether machines are persistent or provisioned, and whether they are shared by multiple users or dedicated to just one user.

Persistent systems have some type of local storage, the contents of which can be expected to persist when the system turns off. Persistent systems may employ storage technology such as storage area networks (SANs) to provide local disk mimicking. In contrast, provisioned systems are created "on the fly" from a base disk and some type of identity disk. Local storage is usually mimicked by a RAM disk or network disk, the latter often provided by a SAN with a high speed link. The provisioning technology is generally Provisioning Services or Machine Creation Services (or a third-party equivalent). Sometimes provisioned systems have persistent local storage, which may be provided by Personal vDisks; these are classed as persistent.

Together, these two factors define the following machine types:

- **Both persistent and dedicated** -- Examples are Desktop OS machines with a static assignment and a Personal vDisk

that are created with Machine Creation Services, desktops with Personal vDisks that are created with VDI-in-a-Box, physical workstations, and laptops

- **Both persistent and shared** -- Examples are Server OS machines that are created with Machine Creation Services
- **Both provisioned and dedicated** -- Examples are Desktop OS machines with a static assignment but without a Personal vDisk that are created with Provisioning Services
- **Both provisioned and shared** -- Examples are Desktop OS machines with a random assignment that are created with Provisioning Services and desktops without Personal vDisks that are created with VDI-in-a-Box

The following Profile management policy settings are suggested guidelines for the different machine types. They work well in most cases, but you may want to deviate from these as your deployment requires.

Important: Delete locally cached profiles on logoff, Profile streaming, and Always cache are enforced by the auto-configuration feature. Adjust the other policies manually.

Persistent machines

Policy	Both persistent and dedicated	Both persistent and shared
Delete locally cached profiles on logoff	Disabled	Enabled
Profile streaming	Disabled	Enabled
Always cache	Enabled (note 1)	Disabled (note 2)
Active write back	Disabled	Disabled (note 3)
Process logons of local administrators	Enabled	Disabled (note 4)

Provisioned machines

Policy	Both provisioned and dedicated	Both provisioned and shared
Delete locally cached profiles on logoff	Disabled (note 5)	Enabled
Profile streaming	Enabled	Enabled
Always cache	Disabled (note 6)	Disabled
Active write back	Enabled	Enabled
Process logons of local administrators	Enabled	Enabled (note 7)

1. Because Profile streaming is disabled for this machine type, the Always cache setting is always ignored.
2. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
3. Disable Active write back except to save changes in profiles of users who roam between XenApp servers. In this case, enable this policy.
4. Disable Process logons of local administrators except for Hosted Shared Desktops. In this case, enable this policy.
5. Disable Delete locally cached profiles on logoff. This retains locally cached profiles. Because the machines are reset at logoff but are assigned to individual users, logons are faster if their profiles are cached.
6. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
7. Enable Process logons of local administrators except for profiles of users who roam between XenApp and XenDesktop servers. In this case, disable this policy.

Folder redirection

Folder redirection lets you store user data on network shares other than the location where the profiles are stored. This reduces profile size and load time but it might impact network bandwidth. Folder redirection does not require that Citrix user profiles are employed. You can choose to manage user profiles on your own, and still redirect folders.

Configure folder redirection using Citrix policies in Studio.

- Ensure that the network locations used to store the contents of redirected folders are available and have the correct permissions. The location properties are validated.
- Redirected folders are set up on the network and their contents populated from users' virtual desktops at logon.

Note: Configure folder redirection using only Citrix Policies or Active Directory Group Policy Objects, not both. Configuring folder redirection using both policy engines may result in unpredictable behavior.

Advanced folder redirection

In deployments with multiple operating systems (OSs), you might want some of a user's profile to be shared by each OS. The rest of the profile is not shared and is used only by one OS. To ensure a consistent user experience across the OSs, you need a different configuration for each OS. This is advanced folder redirection. For example, different versions of an application running on two OSs might need to read or edit a shared file, so you decide to redirect it to a single network location where both versions can access it. Alternatively, because the Start Menu folder contents are structured differently in two OSs, you decide to redirect only one folder, not both. This separates the Start Menu folder and its contents on each OS, ensuring a consistent experience for users.

If your deployment requires advanced folder redirection, you must understand the structure of your users' profile data and determine which parts of it can be shared between OSs. This is important because unpredictable behavior can result unless folder redirection is used correctly.

To redirect folders in advanced deployments:

- Use a separate Delivery Group for each OS.
- Understand where your virtual applications, including those on virtual desktops, store user data and settings, and understand how the data is structured.
- For shared profile data that can safely roam (because it is structured identically in each OS), redirect the containing folders in each Delivery Group.
- For non-shared profile data that cannot roam, redirect the containing folder in only one of the Desktop Groups, typically

the one with the most used OS or the one where the data is most relevant. Alternatively, for non-shared data that cannot roam between OSs, redirect the containing folders on both systems to separate network locations.

Example advanced deployment - This deployment has applications, including versions of Microsoft Outlook and Internet Explorer, running on Windows 8 desktops and applications, including other versions of Outlook and Internet Explorer, delivered by Windows Server 2008. To achieve this, you have already set up two Delivery Groups for the two OSs. Users want to access the same set of Contacts and Favorites in both versions of those two applications.
Important: The following decisions and advice are valid for the OSs and deployment described. In your organization, the folders you choose to redirect and whether your decide to share them depend on a number of factors that are unique to your specific deployment.

- Using policies applied to the Delivery Groups, you choose the following folders to redirect.

Folder	Redirected in Windows 8?	Redirected in Windows Server 2008?
My Documents	Yes	Yes
Application Data	No	No
Contacts	Yes	Yes
Desktop	Yes	No
Downloads	No	No
Favorites	Yes	Yes
Links	Yes	No
My Music	Yes	Yes
My Pictures	Yes	Yes
My Videos	Yes	Yes
Searches	Yes	No
Saved Games	No	No
Start Menu	Yes	No

- For the shared, redirected folders:
  - After analyzing the structure of the data saved by the different versions of Outlook and Internet Explorer, you decide

it is safe to share the Contacts and Favorites folders
    - You know the structure of the My Documents, My Music, My Pictures, and My Videos folders is standard across OSs, so it is safe to store these in the same network location for each Delivery Group
- For the non-shared, redirected folders:
    - You do not redirect the Desktop, Links, Searches, or Start Menu folders folder in the Windows Server Delivery Group because data in these folders is organized differently in the two OSs. It therefore cannot be shared.
    - To ensure predictable behavior of this non-shared data, you redirect it only in the Windows 8 Delivery Group. You choose this, rather than the Windows Server Delivery Group, because Windows 8 will be used more often by users in their day-to-day work; they will only occasionally access the applications delivered by the server. Also, in this case the non-shared data is more relevant to a desktop environment rather than an application environment. For example, desktop shortcuts are stored in the Desktop folder and might be useful if they originate from a Windows 8 machine but not from a Windows Server machine.
- For the non-redirected folders:
    - You do not want to clutter your servers with users' downloaded files, so you choose not to redirect the Downloads folder
    - Data from individual applications can cause compatibility and performance issues, so you decide not to redirect the Application Data folder

For more information on folder redirection, see http://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx.

Folder redirection and exclusions

In Citrix Profile management (but not in Studio), a performance enhancement allows you to prevent folders from being processed using exclusions. If you use this feature, do not exclude any redirected folders. The folder redirection and exclusion features work together, so ensuring no redirected folders are excluded allows Profile management to move them back into the profile folder structure again, while preserving data integrity, if you later decide not to redirect them. For more information on exclusions, see To include and exclude items.

HDX

Sep 29, 2015

Citrix HDX includes a broad set of technologies that provide a high-definition user experience.

At the device	HDX leverages the computing capacity of user devices to enhance and optimize the user experience. HDX MediaStream technology ensures users receive a smooth, seamless experience with multimedia content in their virtual desktops or applications. Workspace control enables users to pause virtual desktops and applications and resume working from a different device at the point where they left off.
On the network	HDX incorporates advanced optimization and acceleration capabilities to deliver the best performance over any network, including low-bandwidth and high-latency WAN connections. HDX features adapt to changes in the environment, balancing performance and bandwidth by applying the best technologies for each unique user scenario, whether the desktop or application is accessed locally on the corporate network or remotely from outside the corporate firewall.
In the datacenter	HDX leverages the processing power and scalability of servers to deliver advanced graphical performance, regardless of the capabilities of the client device. Compressed multimedia information is sent directly to the user device in its native format. HDX channel monitoring provided by Citrix Director displays the status of connected HDX channels on user devices. HDX Insight, the integration of EdgeSight Network Inspector and EdgeSight Performance management with Director, captures data about ICA traffic and provides a dashboard view of real-time and historical details such as client-side and server-side ICA session latency, bandwidth use of ICA channels, and the ICA round trip time value of each session.

To experience HDX capabilities from your virtual desktop:

- See how HDX delivers rich video content to virtual desktops: View a video on a web site containing high definition videos, such as http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.
- See how Flash Redirection accelerates delivery of Flash multimedia content:
  1. Download Adobe Flash player (http://get.adobe.com/flashplayer/) and install it on both the virtual desktop and the user device.
  2. On the Desktop Viewer toolbar, click Preferences. In the Desktop Viewer Preferences dialog box, click the Flash tab and select Optimize content.
  3. To experience how Flash Redirection accelerates the delivery of Flash multimedia content to virtual desktops, view a video on your desktop from a web site containing Flash videos, such as YouTube. Flash Redirection is designed to be seamless so that users do not know when it is running. You can check to see whether Flash Redirection is being used by looking for a block of color that appears momentarily before the Flash player starts.
- See how HDX delivers high definition audio:
  1. Configure your Citrix client for maximum audio quality; see the Receiver documentation for details.
  2. Play music files with a digital audio player (such as iTunes) on your desktop.

HDX provides a superior graphics and video experience for most users by default, with no configuration required. Citrix

policy settings that provide the best out-of-the-box experience for the majority of use cases are enabled by default.

- HDX automatically selects the best delivery method based on the client, platform, application, and network bandwidth, and then self-tunes based on changing conditions.
- HDX optimizes the performance of 2D and 3D graphics and video.
- HDX delivers a Windows Aero experience to virtual desktop users on any client.
- HDX enables user devices to stream multimedia files directly from the source provider on the Internet or Intranet, rather than through the host server. If the requirements for this client-side content fetching are not met, media delivery falls back to Windows Media redirection to play media run-time files on user devices rather than the host server. In most cases, no adjustments to the Windows Media feature policies are needed.

Good to know:

- For support and requirements information for HDX features, see System requirements for XenApp and XenDesktop 7.6. Except where otherwise noted, HDX features are available for supported Windows Server OS and Windows Desktop OS machines, plus Remote PC Access desktops.
- This content describes how to further optimize the user experience, improve server scalability, or reduce bandwidth requirements. For information about working with Citrix policies and policy settings, see the *— Citrix policies* documents for this release.
- For instructions that include working with the registry, use caution: editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Reduce the bandwidth needed for Windows desktops

By default, HDX delivers a highly responsive Windows Aero or Windows 8 desktop experience to virtual desktops accessed from supported Windows user devices. To do that, HDX leverages the graphics processing unit (GPU) or integrated graphics processor (IGP) on the user devices for local DirectX graphics rendering. This feature, named desktop composition redirection, maintains high scalability on the server. For details, see What to do with all these choices in http://blogs.citrix.com/2013/11/06/go-supersonic-with-xendesktop-7-x-bandwidth-supercodecs/.

To reduce the bandwidth required in user sessions, consider adjusting the following Citrix policy settings. Keep in mind that changing these settings can reduce the quality of the user experience.

- **Desktop Composition Redirection**. Applies only to Windows Desktop OS machines accessed from Windows user devices and applies only to the composition of the Windows desktop. Application windows are rendered on the server unless the Citrix policy setting Allow local app access is Allowed.
- **Desktop Composition Redirection graphics quality**. Uses high-quality graphics for desktop composition unless seamless applications or Local App Access are enabled. To reduce bandwidth requirements, lower the graphics quality.
- **Dynamic windows preview**. Controls the display of seamless windows in Flip, Flip 3D, taskbar preview, and peek window preview modes. To reduce bandwidth requirements, disable this policy setting.

Improve the image quality sent to user devices

The following visual display policy settings control the quality of images sent from virtual desktops to user devices.

- Visual quality. Controls the visual quality of images displayed on the user device: medium, high, always lossless, build to lossless (default = medium).
- Target frame rate. Specifies the maximum number of frames per second that are sent from the virtual desktop to the user device (default = 30). In many circumstances, you can improve the user experience by specifying a higher value. For devices with slower CPUs, specifying a lower value can improve the user experience.

- Display memory limit. Specifies the maximum video buffer size for the session in kilobytes (default = 65536 KB). For connections requiring more color depth and higher resolution, increase the limit. You can calculate the maximum memory required. Color depths other than 32-bit are available only if the Legacy graphics mode policy setting is enabled.

Improve video conference performance

HDX webcam video compression improves bandwidth efficiency and latency tolerance for webcams during video conferencing in a session. This technology streams webcam traffic over a dedicated multimedia virtual channel; this uses significantly less bandwidth compared to the isochronous HDX Plug-n-Play support, and works well over WAN connections.

Receiver users can override the default behavior by choosing the Desktop Viewer Mic & Webcam setting Don't use my microphone or webcam. To prevent users from switching from HDX webcam video compression, disable USB device redirection with the policy settings under ICA policy settings > USB Devices policy settings.

HDX webcam video compression is enabled by default on Receiver for Windows but must be configured on Receiver for Linux. For more information, refer to the Receiver documentation. HDX webcam video compression requires that the following policy settings be enabled (all are enabled by default).

- Client audio redirection
- Client microphone redirection
- Multimedia conferencing
- Windows Media Redirection

If a webcam supports H.264 hardware encoding, HDX video compression uses the hardware encoding by default. Hardware encoding uses additional bandwidth and is not suitable for a low bandwidth network. To force software compression over low bandwidth networks, add the following DWORD key value to the registry key: HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

Choose server scalability over user experience

For deployments where server scalability is of greater concern than user experience, you can use the legacy graphics system by adding the Legacy graphics mode policy setting and configuring the individual legacy graphics policy settings. Use of the legacy graphics system affects the user experience over WAN and mobile connections.

Thinwire Compatibility Mode

Oct 17, 2016

This article applies to 7.6 FP3.

Thinwire Compatibility Mode uses new screen decomposition and caching techniques, which achieve low bandwidth usage and high server scalability without compromising the end-user experience.

Thinwire Compatibility Mode includes the following features:

- Intelligent bitmap matching for a bitmap-only provider.
  - Bitmap translation analysis for efficient window movement and scrolling.
- Backwards compatible. There is no requirement for client or Citrix Receiver upgrades or hardware acceleration.
  - Tested on a range of older thin clients up to and over 5 years old.
- Optimized for very low server CPU usage and improved server scalability.
- An emulated 16-bit mode, which reduces bandwidth by a further 15-20% for typical workloads.
- Transient detection for server-rendered video content.
  - Multi-transient handling for an improved multimedia experience. For example, when watching multiple videos or ticker tapes.
  - Selective sharpening for regions that leave a transient state.
- Optimized for CloudBridge acceleration. In tests, we have seen up to a 6:1 ratio of bandwidth reduction on Office-type workloads.
- Adaptive display, which can be tuned through policy settings. For more information see **Moving image compression** in Moving image policy settings.
- VDA's and Windows OS's up to and including Windows 10 VDA are supported.
- New "Build to Lossless" mode for 3D Pro, which improves responsiveness, interactivity, and interruptible sharpening for a better user experience on low bandwidth.
- Default static photographic imagery quality is higher than in Legacy Graphics Mode.

For Visual Quality settings "Low", "Medium" (default) and "High", the transient detector dynamically evaluates screen updates to decide whether highly-animated areas should be sent at lower quality, in accordance with the Adaptive Display policy, to improve client performance and reduce bandwidth usage.

For the **Build to lossless** visual quality, Thinwire Compatibility Mode uses a "fuzzy-first" approach for large screen updates. This setting is targeted at 3D Pro users who are manipulating 3D models or other graphic-intensive applications. If the activity continues, a transient mode is assumed and the affected area is sharpened and cached once transient activity stops. For the initial large change, some lightweight image analysis is performed on the change area to determine whether to use "fuzzy transient" or "sharp transient" (lossless) - for example, when rotating a wireframe. It is more efficient, for FPS (Frames Per Second) and bandwidth, to encode simple imagery using the Citrix lossless codec and no loss in quality occurs.

The sharpen-to-lossless step in Build to lossless is also different. Rather than sharpening the affected area in one step, the area is sharpened in pre-determined blocks to help maintain interactivity and a smooth user experience. Sharpening a large change area mid-transient, for example moving a 3D model which is stopped briefly, then moved again, would previously cause a "stall", especially over a low bandwidth line. The size of the sharpening blocks depends on how far the quality was reduced to try and maintain the target minimum frame rate, which is an Adaptive Display policy setting. If the quality was significantly reduced, the sharpening block size will be smaller, with a minimum size of 128 x 128 pixels. If the quality was not reduced, for example, when the client has adequate processing power and bandwidth, the sharpening block size can be a

maximum size of 384 x 384 pixels.

HDX 3D Pro

Oct 17, 2016

HDX 3D Pro enables you to deliver desktops and applications that perform best with a graphics processing unit (GPU) for hardware acceleration, including 3D professional graphics applications based on OpenGL and DirectX. (The standard VDA supports GPU acceleration of DirectX only.)

Examples of 3D professional applications include:

- Computer-aided design, manufacturing, and engineering (CAD/CAM/CAE) applications
- Geographical Information System (GIS) software
- Picture Archiving Communication System (PACS) for medical imaging
- Applications using the latest OpenGL, DirectX, NVidia CUDA, and OpenCL versions
- Computationally-intensive non-graphical applications that use NVIDIA Compute Unified Device Architecture (CUDA) GPUs for parallel computing

HDX 3D Pro provides the best user experience over any bandwidth:

- On wide area network (WAN) connections: Deliver an interactive user experience over WAN connections with bandwidths as low as 1.5 Mbps.
- On local area network (LAN) connections: Deliver a user experience equivalent to that of a local desktop on LAN connections with bandwidths of 100 Mbps.
  You can replace complex and expensive workstations with simpler user devices by moving the graphics processing into the data center for centralized management.

HDX 3D Pro provides GPU acceleration for Windows Desktop OS machines and Windows Server OS machines. When used with Citrix XenServer and NVIDIA GRID GPUs, HDX 3D Pro provides Virtual GPU (vGPU) acceleration for Windows Desktop OS machines. For the supported XenServer versions, see Citrix Virtual GPU Solution.

Use the HDX Monitor tool (which replaces the Health Check tool) to validate the operation and configuration of HDX visualization technologies and to diagnose and troubleshoot HDX issues. To download the tool and learn more about it, see https://taas.citrix.com/hdx/download/.

Flash Redirection

Sep 29, 2015

Flash Redirection offloads the processing of most Adobe Flash content (including animations, videos, and applications) to users' LAN- and WAN-connected Windows devices, which reduces server and network load. This results in greater scalability while ensuring a high definition user experience. Configuring Flash Redirection requires both server-side and client-side settings.

Caution: Flash Redirection involves significant interaction between the user device and server components. Use this feature only in environments where security separation between the user device and server is not required. Additionally, configure user devices to use this feature only with trusted servers. Because Flash Redirection requires the Flash Player to be installed on the user device, enable this feature only if the Flash Player itself is secured.

The legacy and second generation versions of Flash Redirection are independent solutions and run in separate virtual channels.

- Legacy Flash Redirection features are supported on the client side only. If an earlier version of the Flash Player is installed on the user device, or if the Flash Player cannot be installed, Flash content renders on the server.
- Second generation Flash Redirection is supported on both clients and servers. If the client supports second generation Flash Redirection, Flash content renders on the client. Second generation Flash Redirection features include support for user connections over WAN, intelligent fallback, and a URL compatibility list; see below for details.

Flash Redirection uses Windows event logging on the server to log Flash events. The event log indicates whether Flash Redirection is being used and provides details about issues. The following are common to all events logged by Flash Redirection:

- Flash Redirection reports events to the Application log.
- On Windows 8 and Windows 7 systems, a Flash Redirection-specific log appears in the Applications and Services Logs node.
- The Source value is Flash.
- The Category value is None.

For the latest updates to HDX Flash compatibility, refer to CTX136588.

Configure Flash Redirection on the server

To configure Flash Redirection on the server, use the following Citrix policy settings. For details, see Flash Redirection policy settings.

- Flash default behavior establishes the default behavior of Flash acceleration. By default, Flash Redirection is enabled. To override this default behavior for individual web pages and Flash instances, use the Flash URL compatibility list setting.
- Flash intelligent fallback - detects instances of small Flash movies (such as those frequently used to play advertisements) and renders them on the server instead of redirecting them for rendering on the user device. It does not cause any interruption or failure in the loading of the web page or the Flash application. By default, Flash intelligent fallback is enabled. To redirect all instances of Flash content for rendering on the user device, disable this policy setting.
- Flash server-side content fetching URL list allows you to specify websites whose Flash content can be downloaded to the server and then transferred to the user device for rendering. (By default, Flash Redirection downloads Flash content to the user device, where it is played.) This setting works with (and requires) the Enable server-side content fetching setting on the user device and is intended for use with Intranet sites and internal Flash applications; see below for details. It also works with most Internet sites and can be used when the user device does not have direct access to the Internet (for example, when the XenApp or XenDesktop server provides that connection).
  Note: Server-side content fetching does not support Flash applications using Real Time Messaging Protocols (RTMP); instead, server-side rendering is used, which supports HTTP and HTTPS.

- Flash URL compatibility list - specifies where Flash content from listed websites is rendered: on the user device, on the server, or blocked.
- Flash background color list - enables you to match the colors of web pages and Flash instances, which improves the appearance of the web page when using Flash Redirection.

Configure Flash Redirection on the user device

Install Citrix Receiver and Adobe Flash Player on the user device. No further configuration is required on the user device.

You can change the default settings using Active Directory Group Policy Objects. Import and add the HDX MediaStream Flash Redirection - Client administrative template (HdxFlashClient.adm), which is available in the following folders:

- For 32-bit computers: %Program Files%\Citrix\ICA Client\Configuration\language
- For 64-bit computers: %Program Files (x86)%\Citrix\ICA Client\Configuration\language

The policy settings appear under Administrative Templates > Classic Administrative Templates (ADM) > HDX MediaStream Flash Redirection - Client. See the Microsoft Active Directory documentation for details about GPOs and templates.

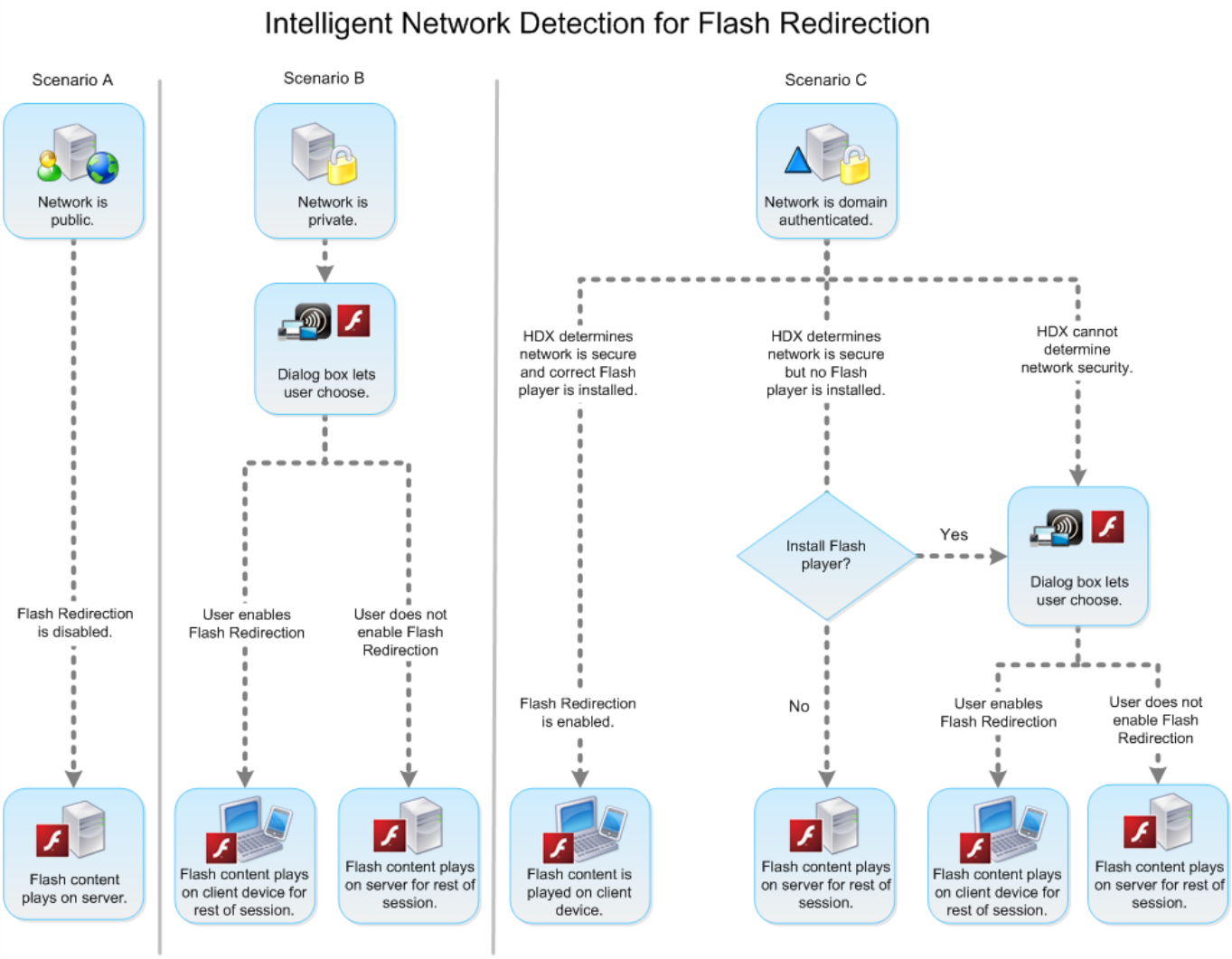
Change when Flash Redirection is used

Together with server-side settings, the Enable HDX MediaStream Flash Redirection on the user device policy setting controls whether Adobe Flash content is redirected to the user device for local rendering. By default, Flash Redirection is enabled and uses intelligent network detection to determine when to play Flash content on the user device.

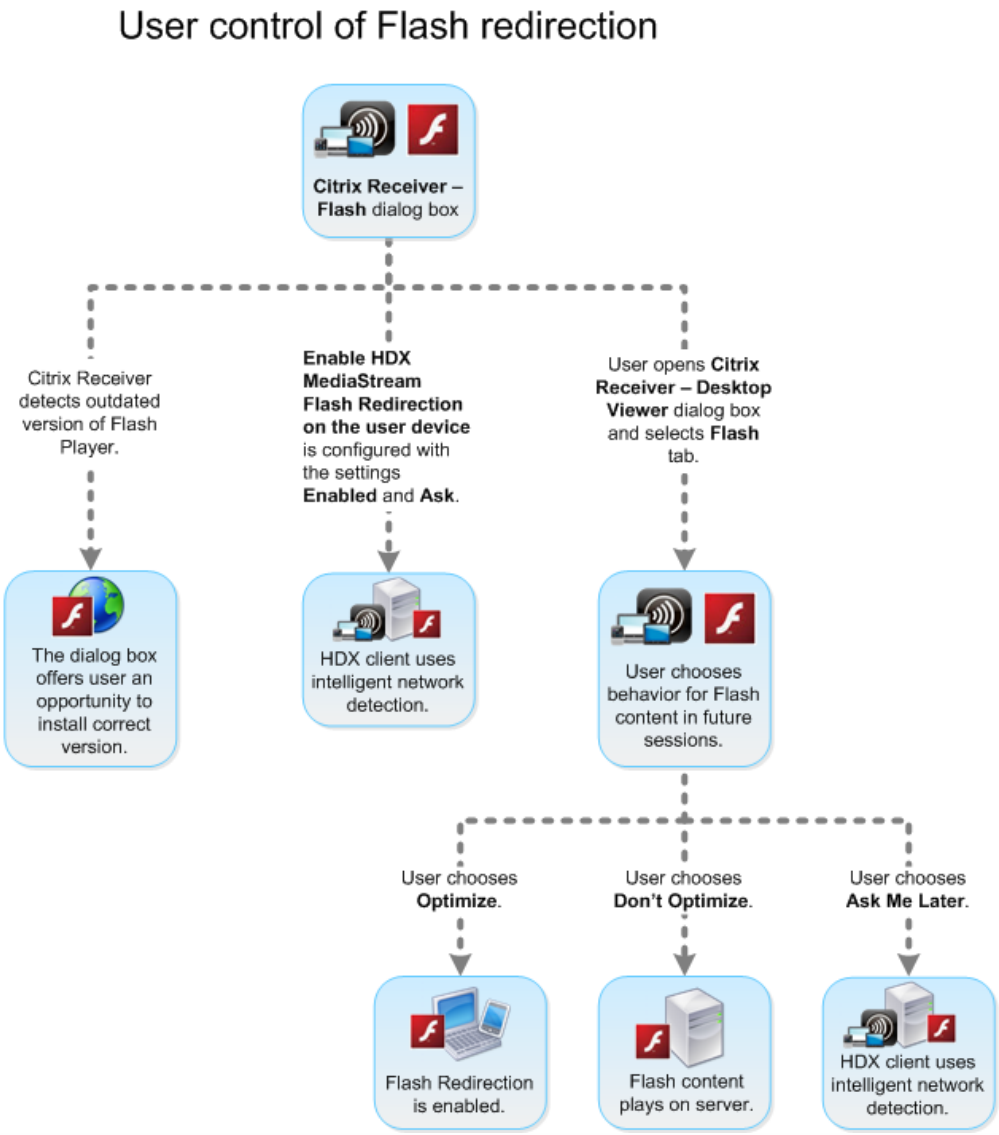
If no configuration is set and Desktop Lock is used, Flash Redirection is enabled on the user device by default.

To change when Flash Redirection is used or to disable Flash Redirection on the user device:

1. From the Setting list, select Enable HDX MediaStream Flash Redirection on the user device and click policy setting.
2. Select Not Configured, Enabled (the default), or Disabled.
3. If you select Enabled, choose an option from the Use HDX MediaStream Flash Redirection list:
   - To use the latest Flash Redirection functionality when the required configuration is present, and revert to server-side rendering when it is not, select Only with Second Generation.
   - To always use Flash Redirection, select Always. Flash content plays on the user device.
   - To never use Flash Redirection, select Never. Flash content plays on the server.
   - To use intelligent network detection to assess the security level of the client-side network to determine when using Flash Redirection is appropriate, select Ask (the default). If the security of the network cannot be determined, the user is asked whether to use Flash Redirection. If the network security level cannot be determined, the user is prompted to choose whether to use Flash Redirection.
     The following illustration indicates how Flash Redirection is handled for various network types.



Users can override intelligent network detection from the Citrix Receiver - Desktop Viewer Preferences dialog box by selecting Optimize or Don't Optimize in the Flash tab. The choices available vary depending on how Flash Redirection is configured on the user device, as shown in the following illustration.



Synchronize client-side HTTP cookies with the server-side

Synchronization of the client-side HTTP cookies with the server-side is disabled by default. Enable synchronization to download HTTP cookies from the server; those HTTP cookies are then used for client-side content fetching and are available as needed by sites containing Flash content.

Note: Client-side cookies are not replaced during the synchronization; they remain available even if the synchronization policy is later disabled.

1. From the Setting list, select Enable synchronization of the client-side HTTP cookies with the server-side and click policy setting.
2. Select Not Configured, Enabled, or Disabled (the default).

Enable server-side content fetching

By default, Flash Redirection downloads Adobe Flash content to the user device, where it is played. Enabling server-side content fetching causes the Flash content to download to the server and then be sent to the user device. Unless there is an overriding policy (such as a site blocked with the Flash URL compatibility list policy setting), the Flash content plays on the user device.

Server-side content fetching is frequently used when the user device connects to internal sites through NetScaler Gateway and when the user device does not have direct access to the Internet.

Note: Server-side content fetching does not support Flash applications using Real Time Messaging Protocols (RTMP). Instead, server-side rendering is used for such sites.
Second generation Flash Redirection supports three enabling options for server-side content fetching. Two of these options include the ability to cache server-side content on the user device, which improves performance because content that is reused is already available on the user device for rendering. The contents of this cache are stored separately from other HTTP content cached on the user device.

With second generation Flash redirection, fallback to server-side content fetching begins automatically when any of the enabling options is selected and client-side fetching of .swf files fails.

Enabling server-side content fetching requires settings on both the client device and the server.

1. From the Setting list, select Enable server-side content fetching and click policy setting.
2. Select Not Configured, Enabled, or Disabled (the default). If you enable this setting, choose an option from the Server-side content fetching state list:

Option	Description
Disabled	Disables server-side content fetching, overriding the Flash server-side content fetching URL list setting on the server. Server-side content fetching fallback is also disabled.
Enabled	Enables server-side content fetching for web pages and Flash applications identified in the Flash server-side content fetching URL list. Server-side content fetching fallback is available, but Flash content is not cached.
Enabled (persistent caching)	Enables server-side content fetching for web pages and Flash applications identified in the Flash server-side content fetching URL list. Server-side content fetching fallback is available. Content obtained through server-side fetching is cached on the user device and stored from session to session.
Enabled (temporary caching)	Enables server-side content fetching for web pages and Flash applications identified in the Flash server-side content fetching URL list. Server-side content fetching fallback is available. Content obtained through server-side fetching is cached on the user device and deleted at the end of the session.

3. On the server, enable the Flash server-side content fetching URL list policy setting and populate it with target URLs.

Redirect user devices to other servers for client-side content fetching

To redirect an attempt to obtain Flash content, use the URL rewriting rules for client-side content fetching setting, which is a second generation Flash Redirection feature. When configuring this feature, you provide two URL patterns; when the user device attempts to fetch content from a website matching the first pattern (the URL match pattern), it is redirected to the website specified by the second pattern (the rewritten URL format).

You can use this setting to compensate for content delivery networks (CDN). Some websites delivering Flash content use CDN redirection to enable the user to obtain the content from the nearest of a group of servers containing the same content. When using Flash Redirection client-side content fetching, the Flash content is requested from the user device, while the rest of the web page on which the Flash content resides is requested by the server. If CDN is in use, the server request is redirected to the nearest server, and the user device request follows to the same location. This may not be the location closest to the user device; depending on distance, there could be a noticeable delay between the loading of the web page and the playing of the Flash content.

1. From the Setting list, select URL rewriting rules for client-side content fetching and click policy setting.
2. Select Not Configured, Enabled, or Disabled. Not Configured is the default; Disabled causes any URL rewriting rules specified in the next step to be ignored.
3. If you enable the setting, click Show. Using Perl regular expression syntax, type the URL match pattern in the Value name box and the rewritten URL format in the Value box.

Minimum version checking for Flash redirection

In XenApp and XenDesktop 7.6 FP3, you can add registry settings to specify the minimum version required for Flash redirection for client devices accessing VDAs using Receiver for Windows or Receiver for Linux.

> **Warning**
>
> Editing the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

ServerFlashPlayerVersionMinimum is a string value that specifies the minimum version of the Flash Player required on the ICA Server (VDA).

ClientFlashPlayerVersionMinimum is a string value that specifies the minimum version of the Flash Player required on the ICA Client (Citrix Receiver).

These version strings can be specified as "10" or "10.2" or "10.2.140". Currently, only the major, minor and build numbers will be compared. The revision number will be ignored. For example, for a version string specified as "10" with only the major number specified, the minor and build numbers will be assumed to be zero.

FlashPlayerVersionComparisonMask is a DWORD value that when set to zero will disable comparing the version of the Flash Player on the ICA Client against the Flash Player on the ICA Server. The comparison mask has other values, but these should not be used because the meaning of any non-zero mask may change. It is recommended to only set the comparison mask to zero for the desired clients. It is not recommended to set the comparison mask under the client agnostic settings. If a comparison mask is not specified, Flash redirection will require that the ICA Client has a Flash Player with greater or equal version to the Flash Player on the ICA Server. It will do so by comparing only the major version number of the Flash Player.

In order for redirection to occur the client and server minimum checks need to be successful in addition to the check using the comparison mask.

The subkey ClientID0x51 specifies the Linux ICA Client. The subkey ClientID0x1 specifies the Windows ICA Client. This subkey is named by appending the hexadecimal Client Product ID (without any leading zeros) to the string "ClientID". A full list of Client IDs can be found in the Mobile SDK for Windows Apps documentation
http://www.citrix.com/mobilitysdk/docs/clientdetection.html

32-bit VDA example registry configuration

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] Client agnostic settings

"ClientFlashPlayerVersionMinimum"="13.0" Minimum version required for the ICA client
"ServerFlashPlayerVersionMinimum"="13.0" Minimum version required for the ICA server
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1] Windows ICA

Client settings

"ClientFlashPlayerVersionMinimum"="16.0.0" This specifies the minimum version of the Flash Player required for the Windows client [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51] Linux ICA Client settings

"FlashPlayerVersionComparisonMask"=dword:00000000 This disables the version comparison-check for the linux client (checking to see that the client has a more recent Flash Player than the server) "ClientFlashPlayerVersionMinimum"="11.2.0" This specifies the minimum version of the Flash Player for the Linux client.

64-bit VDA example registry configuration

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

"ClientFlashPlayerVersionMinimum"="13.0" "ServerFlashPlayerVersionMinimum"="13.0" [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1]

"ClientFlashPlayerVersionMinimum"="16.0.0" [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51]

"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"

Host to client redirection

Oct 17, 2016

Content redirection allows you to control whether users access information with applications published on servers or with applications running locally on user devices.

Host to client redirection is one kind of content redirection. It is supported only on Server OS VDAs (not Desktop OS VDAs).

- When host to client redirection is enabled, URLs are intercepted at the server VDA and sent to the user device. The web browser or multimedia player on the user device opens these URLs.
- If you enable host to client redirection and the user device fails to connect to a URL, the URL is redirected back to the server VDA.
- When host to client redirection is disabled, users open the URLs with web browsers or multimedia players located on the server VDA.
- When host to client redirection is enabled, users cannot disable it.

Host to client redirection was previously known as **server to client redirection**.

When to use host to client redirection

You might consider using host to client redirection in specific but uncommon cases, for performance, compatibility, or compliance. Normally, other forms of content redirection are better.

Performance

You can use host to client redirection for performance, so that whenever an application is installed on the user device, it is used in preference to an application on the VDA.

Keep in mind that host to client redirection will improve performance only under specific conditions, because the VDA already optimizes Adobe Flash and other types of multimedia content. First, consider using the other approaches (policy settings) noted in the tables below, rather than host to client redirection; they offer more flexibility and usually give a better user experience, particularly for less-powerful user devices.

Compatibility

You can use host to client redirection for compatibility in the following use cases:

- You use content types other than HTML or multimedia (for example, a custom URL type).
- You use a legacy media format (such as Real Media) that is not supported by the VDA's multimedia player with multimedia redirection.
- The application for the content type is used by only a small number of users who already have the application installed on their user device.
- The VDA cannot access certain web sites (for example, web sites internal to another organization).

Compliance

You can use host to client redirection for compliance in the following use cases:

- The application or content licensing agreement does not permit publishing via the VDA.

- Organizational policy does not permit a document being uploaded to the VDA.

Some situations are more likely in complex environments, and also if the user device and the VDA belong to different organizations.

User device considerations

Environments may have many different types of user devices.

User device	Situation or environment	Content redirection approach
Tablet	-	Any approach (see next table)
Laptop PC	-	Any approach (see next table)
Desktop PC	Users use a wide range of apps installed on the user device	Any approach (see next table)
Desktop PC	Users use only a few known apps that are installed on the user device	Local App Access
Desktop PC	Users use no apps installed on the user device	Multimedia redirection and/or Flash redirection
Desktop appliance	Vendor supports multimedia redirection and/or Flash redirection	Multimedia redirection and/or Flash redirection
Thin client	Vendor supports multimedia redirection, Flash redirection, and host to client redirection	Any approach (see next table)
Zero client	Vendor supports multimedia redirection and/or Flash redirection	Multimedia redirection and/or Flash redirection

Use the following examples to help guide your content redirection approach.

URLs link	Situation or environment	Content redirection approach
A web page or document	The VDA cannot access the URL	Host to client redirection
A web page	The web page contains Adobe Flash	Flash redirection

A multimedia file or stream	The VDA has a compatible multimedia player	Multimedia redirection
A multimedia file or stream	The VDA does not have a compatible multimedia player	Host to client redirection
A document	The VDA does not have an application for that document type	Host to client redirection
A document	The document must not be downloaded to the user device	No redirection
A document	The document must not be uploaded to the VDA	Host to client redirection
A custom URL type	The VDA does not have an application for that custom URL type	Host to client redirection

Host to client redirection is supported by Citrix Receiver for Windows, Receiver for Mac, Receiver for Linux, Receiver for HTML5, and Receiver for Chrome.

To use host to client redirection, the user device must have a web browser, multimedia player, or other application that is suitable for the content. If the user device is a desktop appliance, thin client, or zero client, confirm that it has suitable applications and is sufficiently powerful.

User devices enabled for Local App Access use a different mechanism for content redirection, and do not require host to client content redirection.

You can use Citrix policies to prevent host to client content redirection for unsuitable devices.

How users experience host to client redirection

Host to client redirection is used when URLs are:

- Embedded as hyperlinks in an application (for example, in an email message or document).
- Selected through a VDA application's menus or dialogs, provided that the application uses the Windows ShellExecuteEx API.
- Entered in the Windows Run dialog.

Host to client redirection is not used for URLs in a web browser (either in a web page or entered in the address bar of the web browser).

> **Note**
>
> If users change their default web browser on the VDA (for example, by using Set Default Programs), that change can interfere with host to client redirection for applications.

When host to client content redirection is enabled, the app that is used to open the URL depends on the configuration of the user device for both the URL type and the content type. For example:

- An HTTP URL with an HTML content type will open in the default web browser.
- An HTTP URL with a PDF content type might open in the default web browser, or it might open in another application.

This user device configuration is not controlled by host to client content redirection. If you do not control the configuration of the user device, consider using Flash redirection and multimedia redirection, rather than host to client content redirection.

The following URL types are opened locally through user devices when host to client redirection is enabled:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- RTSP (Real Player and QuickTime)
- RTSPU (Real Player and QuickTime)
- PNM (Legacy Real Player)
- MMS (Microsoft Media Format)

You can change the list of URL types for host to client redirection, to remove and add URL types, including custom URL types.

Enable host to client redirection

Enabling host to client redirection starts with enabling a Citrix policy setting.

The Host to client redirection policy setting is located in the File Redirection policy settings section. By default, this setting is disabled.

In addition, you may need to set registry keys and Group Policy for the server VDAs, depending on the VDA's OS.

- If the server VDA is Windows Server 2008 R2 SP1, you do not need to set registry keys or Group Policy.
- If the server VDA is Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016, you must set registry keys and Group Policy.

> **Warning**
>
> Using Registry Editor incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Registry changes

1. Copy the text between "**Reg file start"** and "**Reg file end"** below, and paste it in Notepad.
2. Save the Notepad file with "Save As" as type All Files and the name ServerFTA.reg**.**
3. Distribute the **ServerFTA.reg** file to the servers using Active Directory Group Policy.

ServerFTA.reg COPY

```
<p><b>- Reg file start --</b><br>
Windows Registry Editor Version 5.00<br>
 <br>
[HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]<br>
@=&quot;\&quot;C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\&quot; %1&quot;<br>
 <br>
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]<br>
@=&quot;ServerFTA&quot;<br>
 <br>
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]<br>
&quot;ApplicationDescription&quot;=&quot;Server FTA URL.&quot;<br>
&quot;ApplicationIcon&quot;=&quot;C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe,0&quot;<br>
&quot;ApplicationName&quot;=&quot;ServerFTA&quot;<br>
 <br>
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\URLAssociations]<br>
&quot;http&quot;=&quot;ServerFTAHTML&quot;<br>
&quot;https&quot;=&quot;ServerFTAHTML&quot;<br>
 <br>
[HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]<br>
&quot;Citrix.ServerFTA&quot;=&quot;SOFTWARE\\Citrix\\ServerFTA\\Capabilities&quot;<br>
<b>-- Reg file end --</b></p>
```

Group Policy changes

Create an XML file. Copy the text between **"**xml file start" and "xml file end" below, paste it in the XML file, and then save the file as **ServerFTAdefaultPolicy.xml**.

ServerFTAdefaultPolicy.xml COPY

```
<p><b>-- xml file start --</b><br>
&lt;?xml version=&quot;1.0&quot; encoding=&quot;UTF-8&quot;?&gt;<br>
&lt;DefaultAssociations&gt;<br>
&lt;Association Identifier=&quot;http&quot; ProgId=&quot;ServerFTAHTML&quot; ApplicationName=&quot;ServerFTA&quo
&lt;Association Identifier=&quot;https&quot; ProgId=&quot;ServerFTAHTML&quot; ApplicationName=&quot;ServerFTA&qu
&lt;/DefaultAssociations&gt;<br>
<b>-- xml file end --</b></p>
```

From the current Group Policy Management Console, navigate to: **Computer configuration** > **Administrative Templates** > **Windows Components** > **File Explorer** > **Set a default associations configuration file,** and provide the ServerFTAdefaultPolicy.xml file you created.

Change the list of URL types for host to client redirection

To change the list of URL types for host to client redirection, set the following registry key on the server VDA.

Key: HKLM\Software\Wow6432Node\Citrix\SFTA

To remove URL types from the list, set DisableServerFTA and NoRedirectClasses:

Name: DisableServerFTA
Type: REG_DWORD
Data: 1

Name: NoRedirectClasses
Type: REG_MULTI_SZ
Data: Specify any combination of the values: http, https, rtsp, rtspu, pnm, or mms. Enter multiple values on separate lines. For example:

http

https

rtsp

To add URL types to the list, set ExtraURLProtocols:

Name: ExtraURLProtocols
Type: REG_MULTI_SZ
Data: Specify any combination of URL types. Each URL type must include the :// suffix; separate multiple values with semicolons. For example:

customtype1://;customtype2://

Enable host to client redirection for a specific set of web sites

To enable host to client redirection for a specific set of web sites, set the following registry key on the server VDA.

Key: HKLM\Software\Wow6432Node\Citrix\SFTA

Name: ValidSites
Type: REG_MULTI_SZ
Data: Specify any combination of fully-qualified domain names (FQDNs). Enter multiple FQDNs on separate lines. An FQDN may include a wildcard in the leftmost position only. This matches a single level of domain, which is consistent with the rules in RFC 6125. For example:

www.example.com

*.example.com

GPU acceleration for Windows Desktop OS

Feb 05, 2016

With HDX 3D Pro you can deliver graphically intensive applications as part of hosted desktops or applications on Desktop OS machines. HDX 3D Pro supports physical host computers (including desktop, blade, and rack workstations) and XenServer VMs with GPU Passthrough and XenServer VMs with Virtual GPU (vGPU).

Using XenServer GPU Passthrough, you can create VMs with exclusive access to dedicated graphics processing hardware. You can install multiple GPUs on the hypervisor and assign VMs to each of these GPUs on a one-to-one basis.

Using XenServer vGPU, multiple virtual machines can directly access the graphics processing power of a single physical GPU. The true hardware GPU sharing provides full Windows 7 or Windows 2008 R2 SP1 desktops suitable for users with complex and demanding design requirements. Supported for NVIDIA GRID K1 and K2 cards, the GPU sharing uses the same NVIDIA graphics drivers that are deployed on non-virtualized operating systems.

HDX 3D Pro offers the following features:

- Adaptive H.264-based deep compression for optimal WAN and wireless performance. HDX 3D Pro uses CPU-based deep compression as the default compression technique for encoding. This provides optimal compression that dynamically adapts to network conditions.
  The H.264-based deep compression codec no longer competes with graphics rendering for CUDA cores on the NVIDIA GPU. The deep compression codec runs on the CPU and provides bandwidth efficiency.

- Lossless compression option for specialized use cases. HDX 3D Pro also offers a CPU-based lossless codec to support applications where pixel-perfect graphics are required, such as medical imaging. Lossless compression is recommended only for specialized use cases because it consumes significantly more network and processing resources.
  When using lossless compression:
  - The lossless indicator, a system tray icon, notifies the user if the screen displayed is a lossy frame or a lossless frame. This helps when the Visual Quality policy setting specifies Build to lossless. The lossless indicator turns green when the frames sent are lossless.
  - The lossless switch enables the user to change to Always Lossless mode anytime within the session. To select or deselect Lossless anytime within a session, right-click the icon or use the shortcut ALT+SHIFT+1.
    For lossless compression: HDX 3D Pro uses the lossless codec for compression regardless of the codec selected through policy.

    For lossy compression: HDX 3D Pro uses the original codec, either the default or the one selected through policy.

    Lossless switch settings are not retained for subsequent sessions. To use lossless codec for every connection, select Always lossless in the Visual quality policy setting.

- In **7.6 FP3**, you can override the default shortcut, ALT+SHIFT+1, to select or deselect Lossless within a session. Configure a new registry setting at HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Name: HKLM_HotKey, Type: String
  - The format to configure a shortcut combination is C=0|1, A=0|1, S=0|1, W=0|1, K=val. Keys must be comma "," separated. The order of the keys does not matter.
  - A, C, S, W and K are keys, where C=Control, A=ALT, S=SHIFT, W=Win, and K=a valid key. Allowed values for K are 0-9, a-z, and any virtual key code. For more information on virtual key codes, see Virtual-Key Codes on MSDN.
  - For example:
    - For F10, set K=0x79
    - For Ctrl + F10, set C=1, K=0x79
    - For Alt + A, set A=1, K=a or A=1, K=A or K=A, A=1
    - For Ctrl + Alt + 5, set C=1, A=1, K=5 or A=1, K=5, C=1
    - For Ctrl + Shift + F5, set A=1, S=1, K=0x74

    Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

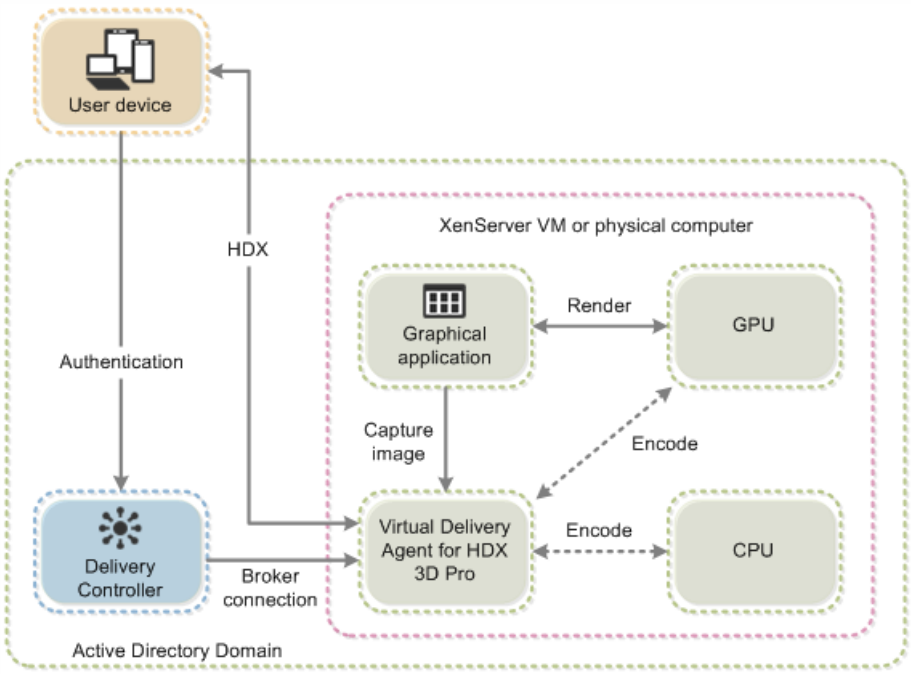
- Multiple and high resolution monitor support. For Windows 7 and Windows 8 desktops, HDX 3D Pro supports user devices with up to four monitors. Users can arrange their monitors in any configuration and can mix monitors with different resolutions and orientations. The number of monitors is limited by the capabilities of the host computer GPU, the user device, and the available bandwidth. HDX 3D Pro supports all monitor resolutions and is limited only by the capabilities of the GPU on the host computer.
  HDX 3D Pro also provides limited support for dual-monitor access to Windows XP desktops. For more information about this, see VDAs on machines running Windows XP or Windows Vista.

- Dynamic resolution. You can resize the virtual desktop or application window to any resolution. **Note**: The only supported method to change the resolution is by resizing the VDA session window. Changing resolution from within the VDA session (using Control Panel > Appearance and Personalization > Display > Screen Resolution) is not supported.
- Support for NVIDIA Kepler architecture. HDX 3D Pro supports NVIDIA GRID K1 and K2 cards for GPU passthrough and GPU sharing. NVIDIA GRID vGPU enables multiple VMs to have simultaneous, direct access to a single physical GPU, using the same NVIDIA graphics drivers that are deployed on non-virtualized operating systems.
- Support for VMware vSphere and VMware ESX using Virtual Direct Graphics Acceleration (vDGA) - You can use HDX 3D Pro with vDGA for both RDS and VDI workloads. When using HDX 3D Pro with Virtual Shared Graphics Acceleration (vSGA), support is limited to one monitor. Using vSGA with large 3D models can result in performance issues due to its use of API intercept technology. For more information, see VMware vSphere 5.1 - Citrix Known Issues.

As shown in the following figure:

- The host computer must reside within the same Active Directory domain as the Delivery Controller.
- When a user logs on to Citrix Receiver and accesses the virtual application or desktop, the Controller authenticates the user and contacts the VDA for HDX 3D Pro to broker a connection to the computer hosting the graphical application.
  The VDA for HDX 3D Pro uses the appropriate hardware on the host to compress views of the complete desktop or of just the graphical application.

- The desktop or application views and the user interactions with them are transmitted between the host computer and the user device through a direct HDX connection between Citrix Receiver and the VDA for HDX 3D Pro.



Install the VDA for HDX 3D Pro

When you use the installer's graphical interface to install a VDA for Windows Desktop OS, simply select Yes on the HDX 3D Pro page. When using the command line interface, include the /enable_hdx_3d_pro option with the XenDesktop VdaSetup.exe command.

To upgrade HDX 3D Pro, uninstall both the separate HDX 3D for Professional Graphics component and the VDA before installing the VDA for HDX 3D Pro. Similarly, to switch from the standard VDA for Windows Desktop OS to the HDX 3D Pro VDA, uninstall the standard VDA and then install the VDA for HDX 3D Pro.

Install and upgrade NVIDIA drivers

The NVIDIA GRID API provides direct access to the frame buffer of the GPU, providing the fastest possible frame rate for a smooth and interactive user experience. If you install NVIDIA drivers before you install a VDA with HDX 3D Pro, NVIDIA

GRID is enabled by default.

To enable NVIDIA GRID on a VM, disable Microsoft Basic Display Adapter from the Device Manager. Run the following command and then restart the VDA: Montereyenable.exe -enable -noreset

If you install NVIDIA drivers after you install a VDA with HDX 3D Pro, NVIDIA GRID is disabled. Enable NVIDIA GRID by using the Montereyenable tool provided by NVIDIA.

To disable NVIDIA GRID, run the following command and then restart the VDA: Montereyenable.exe -disable -noreset

Optimize the HDX 3D Pro user experience

To use HDX 3D Pro with multiple monitors, ensure that the host computer is configured with at least as many monitors as are attached to user devices. The monitors attached to the host computer can be either physical or virtual.

Do not attach a monitor (either physical or virtual) to a host computer while a user is connected to the virtual desktop or application providing the graphical application. Doing so can cause instability for the duration of a user's session.

Let your users know that changes to the desktop resolution (by them or an application) are not supported while a graphical application session is running. After closing the application session, a user can change the resolution of the Desktop Viewer window in the Citrix Receiver - Desktop Viewer Preferences.

When multiple users share a connection with limited bandwidth (for example, at a branch office), Citrix recommends that you use the Overall session bandwidth limit policy setting to limit the bandwidth available to each user. This ensures that the available bandwidth does not fluctuate widely as users log on and off. Because HDX 3D Pro automatically adjusts to make use of all the available bandwidth, large variations in the available bandwidth over the course of user sessions can negatively impact performance.

For example, if 20 users share a 60 Mbps connection, the bandwidth available to each user can vary between 3 Mbps and 60 Mbps, depending on the number of concurrent users. To optimize the user experience in this scenario, determine the bandwidth required per user at peak periods and limit users to this amount at all times.

For users of a 3D mouse, Citrix recommends that you increase the priority of the Generic USB Redirection virtual channel to 0. For information about changing the virtual channel priority, see CTX128190.

GPU acceleration for Windows Server OS

Mar 07, 2016

HDX 3D Pro allows graphics-heavy applications running in Windows Server OS sessions to render on the server's graphics processing unit (GPU). By moving OpenGL, DirectX, Direct3D, and Windows Presentation Foundation (WPF) rendering to the server's GPU, the server's CPU is not slowed by graphics rendering. Additionally, the server is able to process more graphics because the workload is split between the CPU and GPU.

When using HDX 3D Pro, multiple users can share graphics cards. When HDX 3D Pro is used with XenServer GPU Passthrough, a single server hosts multiple graphics cards, one per virtual machine.

For procedures that involve editing the registry, use caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

GPU sharing

GPU Sharing enables GPU hardware rendering of OpenGL and DirectX applications in remote desktop sessions; it has the following characteristics:

- Can be used on bare metal or virtual machines to increase application scalability and performance.
- Enables multiple concurrent sessions to share GPU resources (most users do not require the rendering performance of a dedicated GPU).
- Requires no special settings.

You can install multiple GPUs on a hypervisor and assign VMs to each of these GPUs on a one-to-one basis: either install a graphics card with more than one GPU, or install multiple graphics cards with one or more GPUs each. Mixing heterogeneous graphics cards on a server is not recommended.

Virtual machines require direct passthrough access to a GPU, which is available with Citrix XenServer or VMware vSphere. When HDX 3D Pro is used with GPU Passthrough, each GPU in the server supports one multi-user virtual machine.

GPU Sharing does not depend on any specific graphics card.

- When running on a hypervisor, select a hardware platform and graphics cards that are compatible with your hypervisor's GPU Passthrough implementation. The list of hardware that has passed certification testing with XenServer GPU Passthrough is available at GPU Passthrough Devices.
- When running on bare metal, it is recommended to have a single display adapter enabled by the operating system. If multiple GPUs are installed on the hardware, disable all but one of them using Device Manager.

Scalability using GPU Sharing depends on several factors:

- The applications being run
- The amount of video RAM they consume
- The graphics card's processing power

For example, scalability figures in the range of 8-10 users have been reported on NVIDIA Q6000 and M2070Q cards running applications such as ESRI ArcGIS. These cards offer 6 GB of video RAM. Newer NVIDIA GRID cards offer 8 GB of video RAM and significantly higher processing power (more CUDA cores). With the NVIDIA GRID K2 cards, good performance has been observed with up to 20 users per GRID K2 card. Other applications may scale much higher, achieving 32 concurrent users on a high-end GPU.

Some applications handle video RAM shortages better than others. If the hardware becomes extremely overloaded, this could cause instability or a crash of the graphics card driver. Limit the number of concurrent users to avoid such issues.

To confirm that GPU acceleration is occurring, use a third-party tool such as GPU-Z. GPU-Z is available at http://www.techpowerup.com/gpuz/.

DirectX, Direct3D, and WPF rendering

DirectX, Direct3D, and WPF rendering is only available on servers with a GPU that supports a display driver interface (DDI) version of 9ex, 10, or 11.

- On Windows Server 2008 R2, DirectX and Direct3D require no special settings to use a single GPU.
- On Windows Server 2012, Remote Desktop Services (RDS) sessions on the RD Session Host server use the Microsoft Basic Render Driver as the default adapter. To use the GPU in RDS sessions on Windows Server 2012, enable the Use the hardware default graphics adapter for all Remote Desktop Services sessions setting in the group policy Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment.
- To enable WPF applications to render using the server's GPU, create the following settings in the registry of the server running Windows Server OS sessions:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] "EnableWPFHook"=dword:00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] "EnableWPFHook"=dword:00000001

Experimental GPU acceleration for CUDA or OpenCL applications

Experimental support is provided for GPU acceleration of CUDA and OpenCL applications running in a user session. This support is disabled by default, but you can enable it for testing and evaluation purposes.

To use the experimental CUDA acceleration features, enable the following registry settings:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001

To use the experimental OpenCL acceleration features, enable the following registry settings:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001

OpenGL Software Accelerator

Sep 11, 2015

The OpenGL Software Accelerator is a software rasterizer for OpenGL applications such as ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, CAD, and CAM. In some cases, the OpenGL Software Accelerator can eliminate the need to use graphics cards to deliver a good user experience with OpenGL applications.

Important: The OpenGL Software Accelerator is provided "as is" and must be tested with all applications. It might not work with some applications and is intended as a solution to try if the Windows OpenGL rasterizer does not provide adequate performance. If the OpenGL Software Accelerator works with your applications, it can be used as a way to avoid the cost of GPU hardware.

The OpenGL Software Accelerator is provided in the Support folder on the installation media, and is supported on all valid VDA platforms.

When should you try the OpenGL Software Accelerator?

- If the performance of OpenGL applications running in virtual machines on XenServer or other hypervisors is an issue, try using OpenGL Accelerator. For some applications, the OpenGL Accelerator outperforms the Microsoft OpenGL software rasterizer that is included with Windows because the OpenGL Accelerator leverages SSE4.1 and AVX. OpenGL Accelerator also supports applications using OpenGL versions up to 2.1.
- For applications running on a workstation, first try the default version of OpenGL support provided by the workstation's graphics adapter. If the graphics card is the latest version, in most cases it will deliver the best performance. If the graphics card is an earlier version or does not delivery satisfactory performance, then try the OpenGL Software Accelerator.
- 3D OpenGL applications that are not adequately delivered using CPU-based software rasterization may benefit from OpenGL GPU hardware acceleration. This feature can be used on bare metal or virtual machines.

Audio features

Jan 05, 2016

You can configure and add the following Citrix policy settings to a policy that optimizes HDX audio features. For usage details plus relationships and dependencies with other policy settings, see Audio policy settings and Bandwidth policy settings and Multi-stream connections policy settings.

Important: Most audio features are transported using the ICA stream and are secured in the same way as other ICA traffic. User Datagram Protocol (UDP) audio uses a separate, unsecured, transport mechanism when NetScaler Access Gateway is not in path. If NetScaler Access Gateway is configured to access XenApp and XenDesktop resources, then audio traffic between the endpoint device and NetScaler Access Gateway is secured using DTLS protocol.

Audio quality

In general, higher sound quality consumes more bandwidth and server CPU utilization by sending more audio data to user devices. Sound compression allows you to balance sound quality against overall session performance; use Citrix policy settings to configure the compression levels to apply to sound files.

By default, the Audio quality policy setting is set to High - high definition audio. This setting provides high fidelity stereo audio, but consumes more bandwidth than other quality settings. Do not use this audio quality for non-optimized voice chat or video chat applications (such as softphones), because it may introduce latency into the audio path that is not suitable for real-time communications.

Consider creating separate policies for groups of dial-up users and for those who connect over a LAN or WAN. Over dial-up connections, where bandwidth typically is limited, download speed is often more important to users than sound quality. Therefore, you may want to create one policy for dial-up connections that applies high compression levels to sound, and another for LAN or WAN connections that applies lower compression levels.

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device; see Audio setting policies for user devices.

Client audio redirection

To allow users to receive audio from an application on a server through speakers or other sound devices (such as headphones) on the user device, add the Client audio redirection setting, which is Allowed by default.

Client audio mapping may cause a heavy load on the servers and the network; however, prohibiting client audio redirection disables all HDX audio functionality.

For setting details see Audio policy settings. Remember to enable client audio settings on the user device; see Audio setting policies for user devices.

Client microphone redirection

To allow users to record audio using input devices such as microphones on the user device add the Client microphone redirection setting, which is Allowed by default.

For security, users are alerted when servers that are not trusted by their user devices try to access microphones, and can choose to accept or reject access prior to using the microphone. Users can disable this alert on Citrix Receiver.

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device; see Audio

setting policies for user devices.

Audio Plug N Play

The Audio Plug N Play policy setting allows or prevents the use of multiple audio devices to record and play sound. This setting is Enabled by default.

This setting applies only to Windows Server OS machines.

For setting details, see Audio policy settings.

Audio redirection bandwidth limit and Audio redirection bandwidth limit percent

The Audio redirection bandwidth limit policy setting specifies the maximum bandwidth (in kilobits per second) for a playing and recording audio in a session. The Audio redirection bandwidth limit percent setting specifies the maximum bandwidth for audio redirection as a percentage of the total available bandwidth. By default, zero (no maximum) is specified for both settings. If both settings are configured, the one with the lowest bandwidth limit is used.

For setting details, see Bandwidth policy settings. Remember to enable Client audio settings on the user device; see Audio setting policies for user devices.

Audio over UDP Real-time Transport and Audio UDP port range

By default, **Audio over UDP Real-time Transport** is allowed (when selected at time of installation), opening up a UDP port on the server for connections that use Audio over UDP Real-time Transport. Citrix recommends configuring UDP/RTP for audio, to ensure the best possible user experience in the event of network congestion or packet loss.

Important: Audio data transmitted with UDP is not encrypted when NetScaler Access Gateway is not in path. If NetScaler Access Gateway is configured to access XenApp and XenDesktop resources then audio traffic between the endpoint device and NetScaler Access Gateway is secured using DTLS protocol.

The **Audio UDP port range** specifies the range of port numbers that the Virtual Delivery Agent (VDA) uses to exchange audio packet data with the user device.

By default, the range is 16500 - 16509.

For setting details about Audio over UDP Real-time Transport, see Audio policy settings; for details about Audio UDP port range, see Multi-stream connections policy settings. Remember to enable **Client audio settings** on the user device; see Audio setting policies for user devices.

Audio setting policies for user devices

1. Load the group policy templates by following Configure Receiver with the Group Policy Object template.
2. In the Group Policy Editor, expand Administrative Templates > Citrix Componentes > Citrix Receiver > User Experience.
3. For Client audio settings, select Not Configured, Enabled, or Disabled.
   - **Not Configured**. By default Audio Redirection is enabled with high quality audio or previously configured custom audio settings.
   - **Enabled**. Audio redirection is enabled with selected options.
   - **Disabled**. Audio redirection is disabled.
4. If you select **Enabled**, choose a sound quality. For UDP audio, use Medium (default).
5. For UDP audio only, select **Enable Real-Time Transport** and then set the range of incoming ports to open in the local Windows firewall.

6. To use UDP Audio with NetScaler Access Gateway, select **Allow Real-Time Transport Through gateway**. NetScaler Access Gateway should be configured with DTLS. For more information, see UDP Audio Through a Netscaler Gateway.

As an Administrator, if you do not have control on endpoint devices to make these changes, for example in the case of BYOD or home computers, then use the default.ica attributes from StoreFront to enable UDP Audio.

1. On the StoreFront machine, open C:\inetpub\wwwroot\Citrix\<Store Name>\App_Data\default.ica with an editor such as notepad.
2. Make the entries below under the [Application] section.

```
command
<p>; This is to enable Real-Time Transport</p>
<p>EnableRtpAudio=true</p>
<p>; This is to Allow Real-Time Transport Through gateway</p>
<p>EnableUDPThroughGateway=true</p>
<p>; This is to set audio quality to Medium</p>
<p>AudioBandwidthLimit=1-</p>
<p>; UDP Port range</p>
<p>RtpAudioLowestPort=16500</p>
<p>RtpAudioHighestPort=16509</p>
```

If UDP Audio is enabled by editing default.ica, then UDP audio will enabled for all users who are using that store.

Avoid echo during multimedia conferences

Users in audio or video conferences may hear an echo. Echoes usually occur when speakers and microphones are too close to each other. For that reason, Citrix recommends the use of headsets for audio and video conferences.

HDX provides an echo cancellation option (enabled by default) that minimizes echo. The effectiveness of echo cancellation is sensitive to the distance between the speakers and the microphone; devices should not be too close or too far away from each other.

You can change a registry setting to disable echo cancellation. When working in the registry, use caution: editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Using the Registry Editor on the user device, navigate to one of the following:
   - 32-bit computers: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
   - 64-bit computers: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. Change the Value data field to FALSE.

Network traffic priorities

Sep 29, 2015

Priorities are assigned to network traffic across multiple connections for a session with quality of service (QoS)-supported routers. Four TCP/IP streams (real-time, interactive, background, and bulk) and one UDP/RTP stream (for voice) are available to carry ICA traffic between the user device and the server. Each virtual channel is associated with a specific priority and transported in the corresponding connection. You can set the channels independently, based on the TCP port number used for the connection.

Multiple channel streaming connections are supported for Virtual Delivery Agents (VDAs) installed on Windows 8 and Windows 7 machines. Work with your network administrator to ensure the Common Gateway Protocol (CGP) ports configured in the Multi-Port Policy setting are assigned correctly on the network routers.

Quality of service (QoS) is supported only when multiple session reliability ports, or the CGP ports, are configured.

Caution: Use transport security when using this feature. Citrix recommends using Internet Protocol Security (IPsec) or Secure Sockets Layer (SSL). SSL connections are supported only when the connections traverse a NetScaler Gateway that supports multi-stream. On an internal corporate network, multi-stream connections with SSL are not supported.
To set quality of service for multiple streaming connections, add the following Citrix policy settings to a policy (see Multi-stream connections policy settings for details):

- Multi-Port policy - This setting specifies ports for ICA traffic across multiple connections, and establishes network priorities.
  - Select a priority from the CGP default port priority list; by default, the primary port (2598) has a High priority.
  - Enter additional CGP ports in CGP port1, CGP port2, and CGP port3 as needed, and identify priorities for each. Each port must have a unique priority.

  Explicitly configure the firewalls on VDAs to allow the additional TCP traffic.
- Multi-Stream computer setting - This setting is disabled by default. If you use Citrix Cloudbridge with Multi-Stream support in your environment, you do not need to configure this setting. Configure this policy setting when using third-party routers or legacy Branch Repeaters to achieve the desired Quality of Service (QoS).
- Multi-Stream user setting - This setting is disabled by default.

For policies containing these settings to take effect, users must log off and then log on to the network.

USB and client drive considerations

Sep 29, 2015

Using HDX USB device redirection, a user can connect a flash drive to a local computer and access it remotely from within a virtual desktop or a desktop hosted application. During a session, users can use plug and play devices, including Picture Transfer Protocol (PTP) devices such as digital cameras, Media Transfer Protocol (MTP) devices such as digital audio players or portable media players, and point-of-sale (POS) devices.

Double-hop USB is not supported for desktop hosted application sessions.

USB redirection is available for the Receiver for Windows and the Receiver for Linux.

By default, USB redirection is allowed for certain classes of USB devices, and denied for others; see the Receiver documentation for details. You can restrict the types of USB devices made available to a virtual desktop by updating the list of USB devices supported for redirection.

> ## Important
>
> In environments where security separation between the user device and server is needed, provide guidance to users about the types of USB devices to avoid.

Optimized virtual channels are available to redirect most popular USB devices, and provide performance and bandwidth efficiency over a WAN. The level of support provided depends on the Receiver installed on the user device. Optimized virtual channels are usually the best option, especially in high latency environments.

For USB redirection purposes, the product handles a SMART board the same as a mouse.

The product supports optimized virtual channels with USB 3.0 devices and USB 3.0 ports, such as a CDM virtual channel used to view files on a camera or to provide audio to a headset). The product also supports Generic USB Redirection of USB 3.0 devices connected to a USB 2.0 port.

Specialty devices for which there is no optimized virtual channel are supported by falling back to a Generic USB virtual channel that provides raw USB redirection. For information on USB devices tested with XenDesktop, see CTX123569.

Some advanced device-specific features, such as Human Interface Device (HID) buttons on a webcam, may not work as expected with the optimized virtual channel; if this is an issue, use the Generic USB virtual channel.

Certain devices are not redirected by default, and are available only to the local session. For example, it would not be appropriate to redirect a network interface card that is attached to the user device's system board by internal USB.

The following Citrix policy settings control USB support:

- **Client USB device optimization rules.** Available in **7.6 FP3** using GPMC. The optimization mode is supported for input devices for class=03, for example, signature devices and drawing tablets. If no rule is specified, then the device is handled as Interactive mode (02). Capture mode (04) is the recommended mode for signature devices.
- **Client USB device redirection.** The default is Prohibited.
- **Client USB device redirection rules.** Rules only apply to devices using Generic USB redirection; therefore, the rules do not apply to devices using specialized or optimized redirection, such as CDM.
- **Client USB Plug and Play device redirection.** The default is Allowed, to permit plug-and-play of PTP, MTP, and POS

devices in a user session.

- **Client USB device redirection bandwidth limit.** The default is 0 (no maximum).
- **Client USB device redirection bandwidth limit percent.** The default is 0 (no maximum).

About USB Generic Redirection

Generic USB Redirection is for specialty USB devices for which there is no optimized virtual channel. This functionality redirects arbitrary USB devices from client machines to virtual desktops; with this feature, end users have the ability to interact with a wide selection of generic USB devices in the desktop session as if the devices were physically attached.

With Generic USB Redirection:

- users do not need to install device drivers on the user device
- USB client drivers are installed on the VDA machine

This feature is supported for desktop sessions from VDA for Desktop OS 7.6.

This feature is also supported for desktop sessions from VDA for Server OS 7.6, with these restrictions:

- The VDA machine must be running Windows Server 2012 R2
- Only single-hop scenarios are supported
- The USB client drivers must be compatible with RDSH for Windows 2012 R2
- USB storage devices, audio devices, smartcard reader, and devices that are not fully virtualized are not supported

For more information on configuring Generic USB Redirection, see CTX137939.

Enable USB support

1. Add the Client USB device redirection setting to a policy and set its value to Allowed.
2. (Optional) To update the list of USB devices available for remoting, add the Client USB device redirection rules setting to a policy and specify the USB policy rules.
3. Enable USB support when you install Receiver on user devices. If you specified USB policy rules for the Virtual Delivery Agent in the previous step, specify those same policy rules for Receiver. For thin clients, consult the manufacturer for details of USB support and any required configuration.

Update the list of USB devices available for remoting (Receiver for Windows 4.2)

USB devices are automatically redirected when USB support is enabled and the USB user preference settings are set to automatically connect USB devices. USB devices are also automatically redirected when operating in Desktop Appliance mode and the connection bar is not present. In some instances, however, you might not want to automatically redirect all USB devices. For more information, see CTX123015.

Users can explicitly redirect devices that are not automatically redirected by selecting them from the USB device list. To prevent USB devices from ever being listed or redirected, you can specify device rules on the client and the VDA, as explained below.

You can update the range of USB devices available for remoting by specifying USB device redirection rules for both Receiver and the VDA to override the default USB policy rules.

- Edit the user device registry. An Administrative template (ADM file) is included on the installation media so you can change the user device through Active Directory Group Policy: dvd root \os\lang\Support\Configuration\icaclient_usb.adm.
- Edit the administrator override rules for the Server OS machines through group policy rules. The Group Policy

Management Console is included on the installation media:

- For x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
- For x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

> ## Warning
>
> Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

The product default rules are stored in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. Do not edit these product default rules. Instead, use them as a guide for creating administrator override rules as explained below. The GPO overrides are evaluated before the product default rules.

The administrator override rules are stored in HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. GPO policy rules take the format {Allow:|Deny:} followed by a set of tag=value expressions separated by white space. The following tags are supported:

Tag	Description
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor; see the USB Web site at http://www.usb.org/ for available USB Class Codes
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating new policy rules, note the following:

- Rules are case-insensitive.
- Rules may have an optional comment at the end, introduced by #. A delimiter is not required, and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- White space is used as a separator, but cannot appear in the middle of a number or identifier. For example, Deny: Class = 08 SubClass=05 is a valid rule, but Deny: Class=0 Sub Class=05 is not.
- Tags must use the matching operator =. For example, VID=1230.
- Each rule must start on a new line or form part of a semicolon-separated list.

Important

If you are using the ADM template file, you must create rules on a single line, as a semicolon-separated list.

When working with optimized devices such as mass storage, you usually redirect the device using the specialized CDM channel rather than with policy rules. However, you can override this behavior in one of the following ways:

- Manually redirect optimized device using Generic USB redirection, choose Switch to Generic from the Devices tab of the Preferences dialog box.
- Automatically redirect optimized device using Generic USB redirection, set auto-redirection for storage device (for example, AutoRedirectStorage = 1) and set USB user preference settings to automatically connect USB devices; for more information, see CTX123015.

Examples:

- The following example shows an administrator-defined USB policy rule for vendor and product identifiers:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
       Deny: VID=046D # Deny all Logitech products
```

- The following example shows an administrator-defined USB policy rule for a defined class, sub-class, and protocol:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
      Allow: Class=EF SubClass=01 # Allow Sync devices
      Allow: Class=EF # Allow all USB-Miscellaneous devices
```

Update the list of USB devices available for remoting

By default, USB devices are automatically redirected when USB support is enabled and the USB user preference settings are set to automatically connect USB devices. USB devices are also automatically redirected for Desktop Appliance sites or desktop hosted applications. In some instances, however, you might not want to automatically redirect all USB devices. For more information, see CTX123015.

Desktop Viewer users can redirect devices that are not automatically redirected by selecting them from the USB device list. To prevent USB devices from being listed or redirected, specify device rules on the user device and the VDA.

You can update the range of USB devices available for remoting by specifying USB device redirection rules for both Receiver and the VDA to override the default USB policy rules. Device rules are enforced for both Receiver and the VDA. Be sure to change both so that device remoting works as you intend.

- Edit the user device registry (or the .ini files in the case of the Receiver for Linux). An Administrative template (ADM file) is included on the installation media so you can change the user device through Active Directory Group Policy: dvd root \os\lang\Support\Configuration\icaclient_usb.adm.
- Edit the administrator override rules in the VDA registry on the Server OS machines. An ADM file is included on the installation media so you can change the VDA through Active Directory Group Policy: dvd root \os\lang\Support\Configuration\vda_usb.adm.

Warning

Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be

sure to back up the registry before you edit it.

The product default rules are stored in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. Do not edit these product default rules. Instead, use them as a guide for creating administrator override rules as explained below. The GPO overrides are evaluated before the product default rules.

The administrator override rules are stored in HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. GPO policy rules take the format {Allow:|Deny:} followed by a set of tag=value expressions separated by white space. The following tags are supported:

Tag	Description
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor; see the USB Web site at http://www.usb.org/ for available USB Class Codes
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating new policy rules, note the following:

- Rules are case-insensitive.
- Rules may have an optional comment at the end, introduced by #. A delimiter is not required, and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- White space is used as a separator, but cannot appear in the middle of a number or identifier. For example, Deny: Class = 08 SubClass=05 is a valid rule, but Deny: Class=0 Sub Class=05 is not.
- Tags must use the matching operator =. For example, VID=1230.
- Each rule must start on a new line or form part of a semicolon-separated list.

Important

If you are using the ADM template file, you must create rules on a single line, as a semicolon-separated list.

When working with optimized devices such as mass storage, you usually redirect the device using the specialized CDM channel rather than with policy rules. However, you can override this behavior in one of the following ways:

- Manually redirect optimized device using Generic USB redirection, choose Switch to Generic from the Devices tab of the

Preferences dialog box.

- Automatically redirect optimized device using Generic USB redirection, set auto-redirection for storage device (for example, AutoRedirectStorage = 1) and set USB user preference settings to automatically connect USB devices; for more information, see CTX123015.

Examples:

- The following example shows an administrator-defined USB policy rule for vendor and product identifiers:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
       Deny: VID=046D # Deny all Logitech products
```

- The following example shows an administrator-defined USB policy rule for a defined class, sub-class, and protocol:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
    Allow: Class=EF SubClass=01 # Allow Sync devices
    Allow: Class=EF # Allow all USB-Miscellaneous devices
```

Use and remove USB devices

Users can connect a USB device before or after starting a virtual session.

When using Receiver for Windows, the following apply:

- Devices connected after a session starts appear immediately in the USB menu of the Desktop Viewer.
- If a USB device is not redirecting properly, you can try to resolve the problem by waiting to connect the device until after the virtual session starts.
- To avoid data loss, use the Windows "Safely Remove Hardware" icon before removing the USB device.

USB mass storage devices

For mass storage devices only, remote access is also available through client drive mapping, where the drives on the user device are automatically mapped to drive letters on the virtual desktop when users log on. The drives are displayed as shared folders with mapped drive letters. To configure client drive mapping, use the Client removable drives setting in the File Redirection Policy Settings section of the ICA Policy Settings.

The main differences between the two types of remoting policy are:

Feature	Client drive mapping	Generic USB redirection
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Safe to remove device during a session	No	Yes, provided users follow operating system recommendations for safe removal

If both Generic USB and the client drive mapping policies are enabled and a mass storage device is inserted either before or after a session starts, it will be redirected using client drive mapping. When both Generic USB and the client drive mapping policies are enabled and a device is configured for automatic redirection (see http://support.citrix.com/article/CTX123015) and a mass storage device is inserted either before or after a session starts, it will be redirected using Generic USB.

> **Note**
>
> USB redirection is supported over lower bandwidth connections, for example 50 Kbps, however copying large files will not work.

File access for mapped client drives

You can control whether users can copy files from their virtual environments to their user devices. By default, files and folders on mapped client-drives are available in read/write mode from within the session.

To prevent users from adding or modifying files and folders on mapped client-devices, enable the Read-only client drive access policy setting. When adding this setting to a policy, make sure the Client drive redirection setting is set to Allowed and is also added to the policy.

Monitoring

Apr 24, 2015

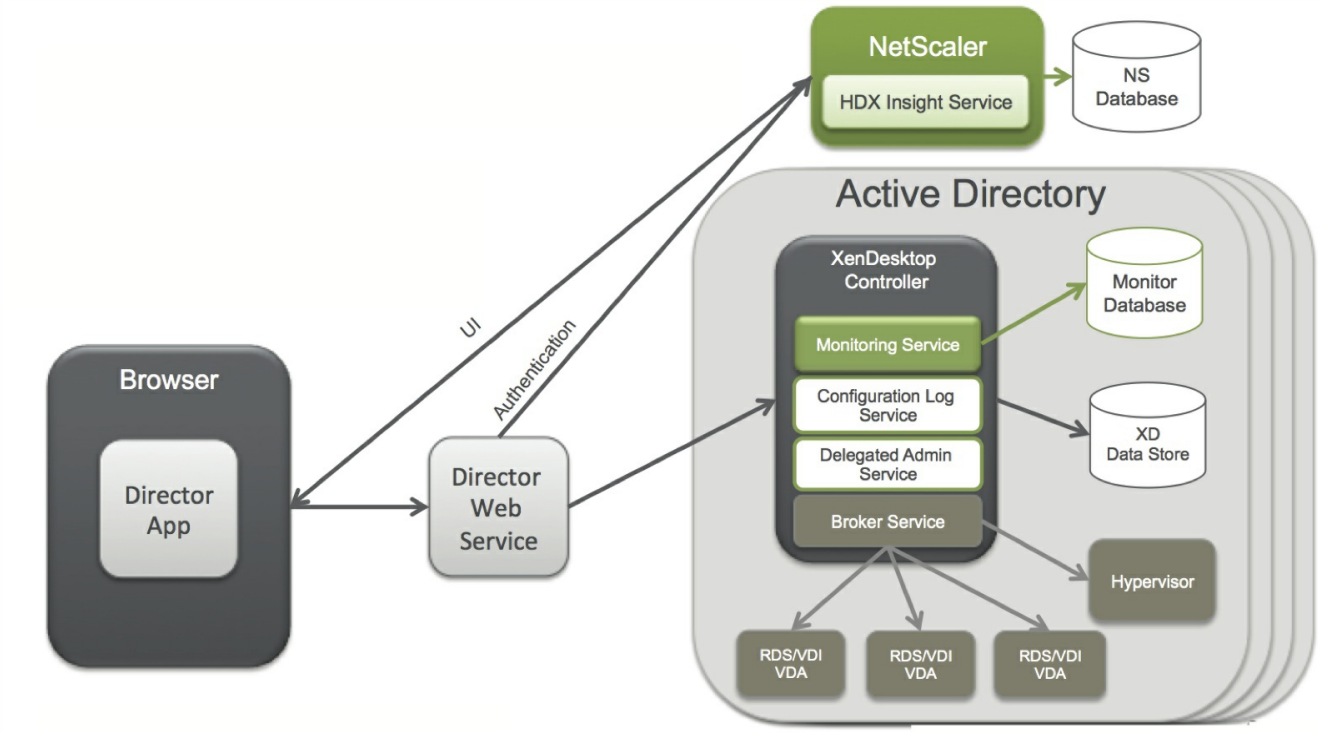
Administrators and help-desk personnel can monitor XenApp and XenDesktop Sites with Director, where administrators can access the Configuration Logging database, or by using the Site's Monitor Service's API using the OData protocol.

Administrators can monitor:

- Session usage
- Logon performance
- Connection and machine failure
- Load evaluation
- Historical trends
- Infrastructure
- User sessions
- Machines

Director

Director is a real-time web tool that allows administrators to monitor, troubleshoot, and perform support tasks for end users.



Director can access:

- Real-time data from the Broker Agent using a unified console integrated with EdgeSight features, Performance Manager, and Network Inspector.
  - EdgeSight features include performance management for health and capacity assurance, and historical trending and network analysis, powered by NetScaler HDX Insight, to identify bottlenecks due to the network in your XenApp or

XenDesktop environment.

- Historical data stored in the Monitor database to access the Configuration Logging database.
- ICA data from the NetScaler Gateway using HDX Insight.
  - Gain visibility into end-user experience for virtual applications, desktops, and users for XenApp or XenDesktop.
  - Correlate network data with application data and real-time metrics for effective troubleshooting.
  - Integrate with XenDesktop 7 Director monitoring tool.
- Personal vDisk Data that allows for runtime monitoring showing base allocation and gives help-desk IT the ability to reset the Personal vDisk (to be used only as a last resort).
  - The command line tool CtxPvdDiag.exe is used to gather the user log information into one file for troubleshooting.

Director uses a troubleshooting dashboard that provides real-time health monitoring of the XenApp or XenDesktop site. This feature allows administrators to see failures in real time, providing a better idea of what the end user is experiencing.

Session Recording - XenApp 7.6 FP1 and FP2 only

Session Recording allows you to record the on-screen activity of any user's session, over any type of connection, from any server running XenApp subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback.

Session Recording uses flexible policies to trigger recordings of application sessions automatically. This enables IT to monitor and examine user activity of applications — such as financial operations and healthcare patient information systems — supporting internal controls for regulatory compliance and security monitoring. Similarly, Session Recording also aids in technical support by speeding problem identification and time-to-resolution.

Configuration Logging

Configuration Logging is a feature that allows administrators to keep track of administrative changes to a XenApp or XenDesktop Site. Configuration Logging can help administrators diagnose and troubleshoot problems after configuration changes are made, assist change management and track configurations, and report administration activity.

Configuration Logging can be viewed in Director with the Trend View interface to provide notifications of configuration changes to administrators who do not have access to XenDesktop Citrix Studio.

Trends View gives historical data of configuration changes over a period of time so administrators can assess what changes were made to the Sites, when they were made, and who made them to find the cause of an issue. This view breaks down configuration information in three categories.

- Connection Failures
- Failed Desktop Machines
- Failed Server Machines

OData API

Administrators can use the Site's Monitor Service's API to search historical data using the OData protocol. This allows IT to analyze historical trends for planning purposes, to perform detailed troubleshooting of connection and machine failures, and extract information for feeding into other tools and processes.

The Monitor Service schema provides the following types of data:

- Data relating to connection failures
- Machines in a failure state

- Session usage
- Logon duration
- Load balancing data

Related content

- Director
- Session Recording - for XenApp 7.6 FP1 and FP2
- Monitor Personal vDisks
- Configuration Logging
- Monitor Service OData API

Director

Oct 14, 2015

Director provides different views of the interface tailored to particular administrators. Product permissions determine what is displayed and the commands available.

For example, help desk administrators see an interface tailored to help desk tasks. Director allows help desk administrators to search for the user reporting an issue and display activity associated with that user, such as the status of the user's applications and processes. They can resolve issues quickly by performing actions such as ending an unresponsive application or process, shadowing operations on the user's machine, restarting the machine, or resetting the user profile.

In contrast, full administrators see and manage the entire site and can perform commands for multiple users and machines. The Dashboard provides an overview of the key aspects of a deployment, such as the status of sessions, user logons, and the site infrastructure. Information is updated every minute. If issues occur, details appear automatically about the number and type of failures that have occurred.

Deploy and configure Director

Director is installed by default as a website on the Delivery Controller. For prerequisites and other details, see the System requirements documentation for this release.

This release of Director is not compatible with XenApp deployments earlier than 6.5 or XenDesktop deployments earlier than 7.

When Director is used in an environment containing more than one Site, be sure to synchronize the system clocks on all the servers where Controllers, Director, and other core components are installed. Otherwise, the Sites might not display correctly in Director.

Tip: If you intend to monitor XenApp 6.5 in addition to XenApp 7.5 or XenDesktop 7.x Sites, Citrix recommends installing Director on a separate server from the Director console that is used to monitor XenApp 6.5 sites.
Important: To protect the security of user names and passwords sent using plain text through the network, Citrix strongly recommends that you allow Director connections using only HTTPS, and not HTTP. Certain tools are able to read plain text user names and passwords in HTTP (unencrypted) network packets, which creates a security risk for users.

To configure permissions

To log on to Director, administrators with permissions for Director must be Active Directory domain users and must have the following rights:

- Read rights in all Active Directory forests to be searched (see Advanced configuration).
- Configured Delegated Administrator roles (see Delegated Administration and Director).
- To shadow users, administrators must be configured using a Microsoft group policy for Windows Remote Assistance. In addition:
  - When installing VDAs, ensure the Windows Remote Assistance feature is enabled on all user devices (selected by default).
  - When you install Director on a server, ensure that Windows Remote Assistance is installed (selected by default). However, it is disabled on the server by default. The feature does not need to be enabled for Director to provide assistance to end users. Citrix recommends leaving the feature disabled to improve security on the server.
  - To enable administrators to initiate Windows Remote Assistance, grant them the required permissions by using the appropriate Microsoft Group Policy settings for Remote Assistance. For information, see CTX127388: How to Enable

Remote Assistance for Desktop Director.

- For user devices with VDAs earlier than 7, additional configuration is required. See Configure permissions for VDAs earlier than XenDesktop 7.

To install Director

Note: To allow Director to find all the XenApp workers in the farm, you will need to add a reverse DNS zone for the subnets where the XenApp servers reside on the DNS servers used by the farm.

Install Director using the installer, which checks for prerequisites, installs any missing components, sets up the Director website, and performs basic configuration. The default configuration provided by the installer handles typical deployments. If Director was not included during installation, use the installer to add Director. To add any additional components, rerun the installer and select the components to install. For information on using the installer, see the Installation documentation. Citrix recommends that you install using the product installer only, not the .MSI file.

When Director is installed on the Controller, it is automatically configured with localhost as the server address, and Director communicates with the local controller by default.

To install Director on a dedicated server that is remote from a Controller, you are prompted to enter the FQDN or IP address of a Controller. Director communicates with that specified Controller by default. Specify only one Controller address for each Site that you will monitor. Director automatically discovers all other Controllers in the same Site and falls back to those other Controllers if the Controller you specified fails.

Note: Director does not load balance between Controllers.
To secure the communications between the browser and the Web server, Citrix recommends that you implement SSL on the IIS website hosting Director. Refer to the Microsoft IIS documentation for instructions. Director configuration is not required to enable SSL.

To install Director 7.6.300

Director 7.6.300 provides support for the Framehawk virtual channel and delivers the latest product fixes. It is available with XenApp and XenDesktop 7.6 FP2 and with XenApp 6.5 FP3.

Note: Check that you have selected all the required features in IIS. For the full list, see CTX142260.

1. Download Director, and run the MSI file, DesktopDirector.MSI or DesktopDirector_x64.MSI.
2. Install CitrixGroupPolicyManagement.MSI, which is available in the Citrix Policy folder on the XenApp and XenDesktop installation media.
3. Configure Director with the Delivery Controller, use the DirectorConfig.exe tool available in C:\inetpub\wwwroot\Director\tools. For more information, see CTX137990.
4. Register ASP.net with IIS. To do this, run the command C:\inetpub\wwwroot\Director\tools>DirectorConfig.exe /registerdotnet
5. Install or upgrade the WMIProxy on the VDA, and restart the machine. WMIProxy_x64.MSI and WIMIProxy_x86.MSI are included in the Director 7.6.300 download files. **Note**: The Framehawk virtual channel will be shown as “Not Compatible” with a VDA with Framehawk enabled, if the WMIProxy is not upgraded.
6. Upgrade XDPoshSnapin_Hotfix on the Delivery Controller, then restart Studio. XDPoshSnapin MSI is available with the Director files downloaded in step 1. This is required for Delegated Administrators and Custom Administrators to view the Framehawk virtual channel information.

To log on to Director

The Director website is located at https or http://<Server_FQDN>/Director.

If one of the Sites in a multi-site deployment is down, the logon for Director takes a little longer while it attempts to connect to the Site that is down.

To install Director for XenApp 6.5

If Director is already installed for XenDesktop, complete the configuration for XenApp as follows:

- Use the IIS Manager Console on each Director server to update the list of XenApp server addresses in the application settings as described in the " To add sites to Director" section in Advanced configuration. Supply the server address of one controller per XenApp farm: Any of the other controllers in a XenApp farm are then used automatically for failover. Director does not load balance between controllers.
- Configure each XenApp worker server to accept WinRM queries as described in Configure permissions.
- Configure a firewall exception for port 2513, used for communication between Director and XenApp.

To install Director for XenApp 6.5 for the first time

To install Director for XenApp 6.5 for the first time, follow these steps. Typically, Director is installed on a separate computer from the XenApp controllers.

1. Install Director from the XenApp 7.6 installation media.
2. Use the IIS Manager Console on each Director server to update the list of XenApp server addresses in the application settings as described in the " To add sites to Director" section in Advanced configuration.
   Supply the server address of one controller per XenApp site: any of the other controllers in a XenApp site are then used automatically for failover. Director does not load balance between controllers.

   Important: For XenApp addresses, be sure to use the setting Service.AutoDiscoveryAddressesXA, not the default setting Service.AutoDiscoveryAddresses.
3. The Director WMI provider installer is at Support\DirectorWMIProvider folder on the DVD. Install it on all appropriate XenApp servers (controllers and workers where sessions are running).
   If winrm is not configured, run the winrm qc command.
4. Configure each XenApp worker server to accept WinRM queries as described in Configure permissions.
5. Configure a firewall exception for port 2513, used for communication between Director and XenApp.
6. To secure the communications between the browser and the web server, Citrix recommends that you implement SSL on the IIS web site hosting Director.
   Refer to the Microsoft IIS documentation for instructions. No Director configuration is required to enable SSL.

Delegated Administration and Director

Apr 27, 2015

Delegated Administration uses three concepts: administrators, roles, and scopes. Permissions are based on an administrator's role and the scope of this role. For example, an administrator might be assigned a Help Desk administrator role where the scope involves responsibility for end-users at one site only.

For information about creating delegated administrators, see the main Delegated Administration document.

Administrative permissions determine the Director interface presented to administrators and the tasks they can perform. Permissions determine:

- The views the administrator can access, collectively referred to as a view.
- The desktops, machines, and sessions that the administrator can view and interact with.
- The commands the administrator can perform, such as shadowing a user's session or enabling maintenance mode.

The built-in roles and permissions also determine how administrators use Director:

Administrator Role	Permissions in Director
Full Administrator	Full access to all views and can perform all commands, including shadowing a user's session, enabling maintenance mode, and exporting trends data.
Delivery Group Administrator	Full access to all views and can perform all commands, including shadowing a user's session, enabling maintenance mode, and exporting trends data.
Read Only Administrator	Can access all views and see all objects in specified scopes as well as global information. Can download reports from HDX channels and can export Trends data using the Export option in the Trends view. Cannot perform any other commands or change anything in the views.
Help Desk Administrator	Can access only the Help Desk and User Details views and can view only objects that the administrator is delegated to manage. Can shadow a user's session and perform commands for that user. Can perform maintenance mode operations. Can use power control options for Desktop OS Machines. Cannot access the Dashboard, Trends, or Filters views. Cannot use power control options for Server OS machines.
Machine Catalog Administrator	No access. This administrator is not supported for Director and cannot view data. This user can access the Machine Details page (Machine-based search).
Host Administrator	No access. This administrator is not supported for Director and cannot view data.

To configure custom roles for Director administrators

In Studio, you can also configure Director-specific, custom roles to more closely match the requirements of your organization and delegate permissions more flexibly. For example, you can restrict the built-in Help Desk administrator role so that this administrator cannot log off sessions.

If you create a custom role with Director permissions, you must also give that role other generic permissions:

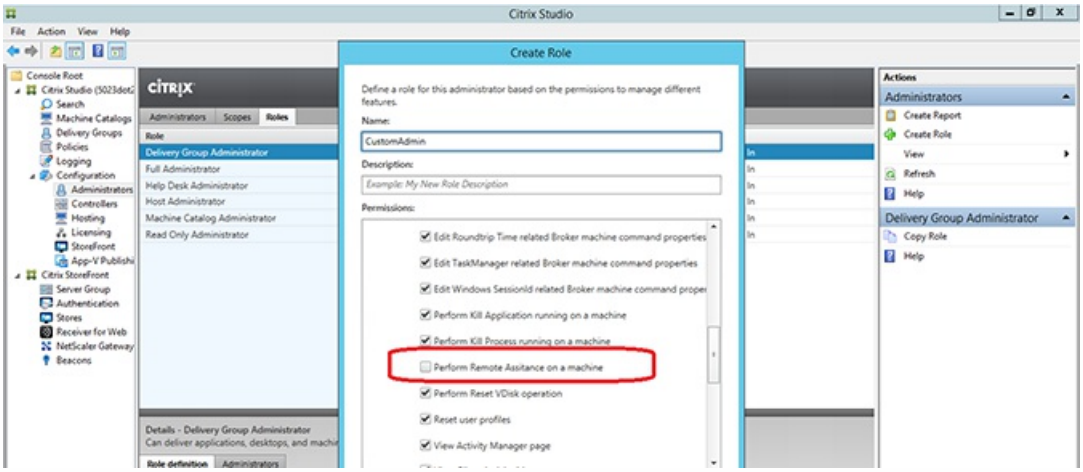
- Delivery Controller permission to log on to Director.
- Permissions to Delivery Groups to view the data related to those Delivery Groups in Director.

Alternatively, you can create a custom role by copying an existing role and include additional permissions for different views. For example, you can copy the Help Desk role and include permissions to view the Dashboard or Filters pages.

Select the Director permissions for the custom role, which include:

- Perform Kill Application running on a machine
- Perform Kill Process running on a machine
- Perform Remote Assistance on a machine
- Perform Reset vDisk operation
- Reset user profiles
- View Client Details page
- View Dashboard page
- View Filters page
- View Machine Details page
- View Trends page
- View User Details page

In this example, Shadowing (Perform Remote Assistance on a machine) is turned off.



In addition, from the list of permissions for other components, consider these permissions:

- From Delivery Groups:
  - Enable/disable maintenance mode of a machine using Delivery Group membership
  - Perform power operations on Windows Desktop machines using Delivery Group membership
  - Perform session management on machines using Delivery Group membership

Configure permissions for VDAs earlier than XenDesktop 7

Apr 27, 2015

If users have VDAs earlier than XenDesktop 7 installed on their devices, Director supplements information from the deployment with real-time status and metrics through Windows Remote Management (WinRM).

In addition, use this procedure to configure WinRM for use with Remote PC in XenDesktop 5.6 Feature Pack1.

By default, only local administrators of the desktop machine (typically domain administrators and other privileged users) have the necessary permissions to view the real-time data.

For information about installing and configuring WinRM, see CTX125243.

To enable other users to view the real-time data, you must grant them permissions. For example, suppose there are several Director users (HelpDeskUserA, HelpDeskUserB, and so on) who are members of an Active Directory security group called HelpDeskUsers. The group has been assigned the Help Desk administrator role in Studio, providing them with the required Delivery Controller permissions. However, the group also needs access to the information from the desktop machine.

To provide the necessary access, you can configure the required permissions in one of two ways:

- Grant permissions to the Director users (impersonation model)
- Grant permissions to the Director service (trusted subsystem model)

To grant permissions to the Director users (impersonation model)

By default, Director uses an impersonation model: The WinRM connection to the desktop machine is made using the Director user's identity. It is therefore the user that must have the appropriate permissions on the desktop.

You can configure these permissions in one of two ways (described later in this document):

1. Add users to the local Administrators group on the desktop machine.
2. Grant users the specific permissions required by Director. This option avoids giving the Director users (for example, the HelpDeskUsers group) full administrative permissions on the machine.

To grant permissions to the Director service (trusted subsystem model)

Instead of providing the Director users with permissions on the desktop machines, you can configure Director to make WinRM connections using a service identity and grant only that service identity the appropriate permissions.

With this model, the users of Director have no permissions to make WinRM calls themselves. They can only access the data using Director.

The Director application pool in IIS is configured to run as the service identity. By default, this is the APPPOOL\Director virtual account. When making remote connections, this account appears as the server's Active Directory computer account; for example, MyDomain\DirectorServer$. You must configure this account with the appropriate permissions.

If multiple Director websites are deployed, you must place each web server's computer account into an Active Directory security group that is configured with the appropriate permissions.

To set Director to use the service identity for WinRM instead of the user's identity, configure the following setting, as

described in Advanced configuration:

```
Service.Connector.WinRM.Identity = Service
```

You can configure these permissions in one of two ways:

1. Add the service account to the local Administrators group on the desktop machine.
2. Grant the service account the specific permissions required by Director (described next). This option avoids giving the service account full administrative permissions on the machine .

To assign permissions to a specific user or group

The following permissions are required for Director to access the information it requires from the desktop machine through WinRM:

- Read and execute permissions in the WinRM RootSDDL
- WMI namespace permissions:
  - root/cimv2 — remote access
  - root/citrix — remote access
  - root/RSOP — remote access and execute
- Membership of these local groups:
  - Performance Monitor Users
  - Event Log Readers

The ConfigRemoteMgmt.exe tool, used to automatically grant these permissions, is on the installation media in the x86\Virtual Desktop Agent and x64\Virtual Desktop Agent folders and on the installation media in the tools folder. You must grant permissions to all Director users.

To grant the permissions to an Active Directory security group, user, computer account, or for actions like End Application and End Process, run the tool with administrative privileges from a command prompt using the following arguments:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name
```

where name is a security group, user, or computer account.

To grant the required permissions to a user security group:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
```

To grant the permissions to a specific computer account:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
```

For End Process, End Application, and Shadow actions:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
```

To grant the permissions to a user group:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all
```

To display help for the tool:

```
ConfigRemoteMgmt.exe
```

Configure HDX Insight

Jul 02, 2014

Note: The availability of this feature depends on your organization's license and your administrator permissions.

HDX Insight is the integration of EdgeSight network analysis and EdgeSight performance management with Director:

- EdgeSight network analysis leverages HDX Insight to provide an application and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in their deployment.
- EdgeSight performance management provides the historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

After you enable this feature in Director, HDX Insight provides Director with additional information:

- The Trends page shows latency and bandwidth effects for applications, desktops, and users across the entire deployment.
- The User Details page shows latency and bandwidth information specific to a particular user session.

Limitations

- ICA session Round Trip Time (RTT) shows data correctly for Receiver for Windows 3.4 or higher and the Receiver for Mac 11.8 or higher. For earlier versions of these Receivers, the data does not display correctly.
- In the Trends view, HDX connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.

To configure the EdgeSight network analysis feature on Director

EdgeSight provides network analysis by leveraging NetScaler HDX Insight to provide the Citrix application and desktop administrators the ability to troubleshoot and correlate issues that can be attributed to poor network performance.

NetScaler Insight Center must be installed and configured in Director to enable EdgeSight network analysis. Insight Center is a virtual machine (appliance) downloaded from Citrix.com. Using EdgeSight network analysis, Director communicates and gathers the information that is related to your deployment. This information is leveraged from HDX Insight, which provides robust analysis of the Citrix ICA protocol between the client and the back-end Citrix infrastructure.

1. On the server where Director is installed, locate the DirectorConfig command line tool in C:\inetpub\wwwroot\Director\tools, and run it with parameter /configNetScaler in command line prompt.
2. When prompted, configure the NetScaler Insight Center machine name (FQDN or IP address), username, password, and HTTP or HTTPS connection type.
3. To verify the changes, log off and log back on.

Advanced configuration

Oct 28, 2015

In this article:

Some advanced Director configuration, such as supporting multiple sites or multiple Active Directory forests, is controlled through settings in Internet Information Services (IIS) Manager.
Important: When you change a setting in IIS, the Director service automatically restarts and logs off users.
To configure advanced settings using IIS:

1. Open the Internet Information Services (IIS) Manager console.
2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.
4. Double-click a setting to edit it.

Platinum licenses retain data for 90 days by default. For more information on configurations see, Data granularity and retention.

To support users across multiple Active Directory domains and forests

Director uses Active Directory to search for users and to look up additional user and machine information. By default, Director searches the domain or forest in which:

- The administrator's account is a member.
- The Director web server is a member (if different).

Director attempts to perform searches at the forest level using the Active Directory global catalog. If the administrator does not have permissions to search at the forest level, only the domain is searched.

To search or look up data from another Active Directory domain or forest requires that you explicitly set the domains or forests to be searched. Configure the following setting:
`Connector.ActiveDirectory.Domains = (user),(server)`
The value attributes user and server represent the domains of the Director user (the administrator) and Director server respectively.

To enable searches from an additional domain or forest, add the name of the domain to the list, as shown in this example:

`Connector.ActiveDirectory.Domains = (user),(server),<domain1>,<domain2>`
For each domain in the list, Director attempts to perform searches at the forest level. If the administrator does not have permissions to search at the forest level, only the domain is searched.

To add sites to Director

If Director is already installed, configure it to work with multiple sites. To do this, use the IIS Manager Console on each

Director server to update the list of server addresses in the application settings.

Add an address of a controller from each site to the following setting:
`Service.AutoDiscoveryAddresses = SiteAController,SiteBController`
where SiteAController and SiteBController are the addresses of Delivery Controllers from two different sites.

For XenApp 6.5 sites, add an address of a controller from each XenApp farm to the following setting:
`Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController`
where FarmAController and FarmBController are the addresses of XenApp controllers from two different farms.

For XenApp 6.5 sites, another way to add a controller from a XenApp farm:
`DirectorConfig.exe /xenapp FarmControllerName`

To disable the visibility of running applications in the Activity Manager

By default, the Activity Manager in Director displays a list of all the running applications for the user's session. This information can be viewed by all administrators that have access to the Activity Manager feature in Director. For Delegated Administrator roles, this includes Full administrator, Delivery Group administrator, and Help Desk Administrator.

To protect the privacy of users and the applications they are running, you can disable the Applications tab from listing running applications.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. On the VDA, modify the registry key located at HKLM\Software\Citrix\Director\TaskManagerDataDisplayed. By default, the key is set to 1. Change the value to 0, which means the information will not be displayed in the Activity Manager.
2. On the server with Director installed, modify the setting that controls the visibility of running applications. By default, the value is true, which allows visibility of running applications in the Applications tab. Change the value to false, which disables visibility. This option affects only the Activity Manager in Director, not the VDA.
   Modify the value of the following setting:
   `UI.TaskManager.EnableApplications = false`

Important: To disable the view of running applications, Citrix recommends making both changes to ensure the data is not displayed in Activity Manager.

Monitor deployments

Nov 21, 2016

With full administrator permissions, when you open Director, the Dashboard provides a centralized location to monitor the health and usage of a site.

If there are currently no failures and no failures have occurred in the past 60 minutes, panels stay collapsed. When there are failures, the specific failure panel automatically appears.

Note: Depending on your organization's license and your Administrator privileges, some options or features might not be available.

Panel	Description
User Connection Failures	Connection failures over the last 60 minutes. Click the categories next to the total number to view metrics for that type of failure. In the adjacent table, that number is broken out by Delivery Groups.
Failed Desktop OS Machines or Failed Server OS Machines	Total failures in the last 60 minutes broken out by Delivery Groups. Failures broken out by types, including failed to start, stuck on boot, and unregistered. For Server OS machines, failures also include machines reaching maximum load.
Licensing Status	• License Server alerts are sent by the License Server and also display the actions required to resolve the alert. • Delivery Controller alerts display the details of the licensing state as seen by the controller and are sent by the Delivery Controller. You can set the threshold for alerts in Studio. License Server and/or Delivery Controller alerts do not display if your License Server version is earlier than 11.12.1 and/or your Delivery Controller is older than XenApp 7.6 or XenDesktop 7.6.
Sessions Connected	Connected sessions across all Delivery Groups for the last 60 minutes.
Average Logon Duration	Logon data for the last 60 minutes. The large number on the left is the average logon duration across the hour. Logon data for VDAs earlier than XenDesktop 7.0 is not included in this average.
Infrastructure	Health status of your site's hosts, controllers. and infrastructure. View performance alerts. For hosts, the connection status and the health of the CPU, memory, bandwidth (network usage), and storage (disk usage) are monitored using information from XenServer or VMware. For example, you can configure XenCenter to generate performance alerts when CPU, network I/O or disk I/O usage go over a specified threshold on a managed server or virtual machine. By default, the alert repeat interval is 60 minutes, but you can configure this as well. For details, in the XenServer

Panel	Description

documentation, see Configuring Performance Alerts.

Note: If no icon appears for a particular metric, this indicates that this metric is not supported by the type of host you are using. For example, no health information is available for System Center Virtual Machine Manager (SCVMM) hosts, AWS and CloudStack.

Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

Monitor sessions

If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the server.

Action	Description
View a user's currently connected machine or session	From the Activity Manager and User Details views, view the user's currently connected machine or session and a list of all machines and sessions to which this user has access. To access this list, click the session switcher icon in the user title bar. See Restore sessions.
View the total number of connected sessions across all Delivery Groups	From the Dashboard, in the Sessions Connected pane, view the total number of connected sessions across all Delivery Groups for the last 60 minutes. Then click the large total number, which opens the Filters view, where you can display graphical session data based on selected Delivery Groups and ranges and usage across Delivery Groups.
View data over a longer period of time	On the Trends view, select the Sessions tab to drill down to more specific usage data for connected and disconnected sessions over a longer period of time (that is, session totals from earlier than the last 60 minutes). To view this information, click View historical trends.

Note: If the user device is running a legacy Virtual Delivery Agents (VDA), such as a VDA earlier than version 7, Director cannot display complete information about the session. Instead, it displays a message that the information is not available in the User Details view and Activity Manager panel.

Filter data to troubleshoot failures

When you click numbers on the Dashboard or select a predefined filter from the Filter menu, the Filter view opens to display the data based on the selected machine or failure type.

Predefined filters cannot be edited, but you can save a predefined filter as a custom filter and then modify it. Additionally, you can create custom filtered views of machines, connections, and sessions across all Delivery Groups.

1. Select a view:
   - Machines — Select Desktop OS Machines or Server OS Machines. These views show the number of configured machines. The Server OS Machines tab also includes the load evaluator index, which indicates the distribution of performance counters and tool tips of the session count if you hover over the link.
   - Sessions — You can also see the session count from the Machines view.

- Connections — Filter connections by different time periods, including last 60 minutes, last 24 hours, or last 7 days.

2. For Failure by, select the criteria.
3. Use the additional tabs for each view, as needed, to complete the filter.
4. Select additional columns, as needed, to troubleshoot further.
5. Save and name your filter.
   To open filter later, from the Filter menu, select the failure type (Machines, Sessions, or Connections), and then select the saved filter.
6. If needed, for Machines or Connections views, use power controls for all the machines you select in the filtered list. The failure reasons and recommended actions for the Machine and Connection failures are available in Citrix Director 7.6 Failure Reasons Troubleshooting Guide.
7. For the Sessions view, use the session controls or option to send messages.

Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

Monitor historical trends across a site - Feature Pack 1

The Trends view accesses historical trend information for sessions, connection failures, machine failures, logon performance, and load evaluation for each site. To locate this information, click from the Dashboard or Filtersview, click Trends.

The zoom-in drilldown feature lets you navigate through trend charts by zooming in on a time period (clicking on a data point in the graph) and drilling down to see the details associated with the trend. This feature enables you to better understand the details of who or what has been affected by the trends being displayed.

To change the default scope of each graph, apply a different filter to the data.

Action	Description
Export graph data	Select the tab containing the data to export. Click Export and select the file format: .PDF, Excel, or .CSV.
View trends for sessions	From the Sessions tab, select the Delivery Group and time period to view more detailed information about the concurrent session count.
View trends for connection failures	From the Connection Failures tab, select the machine type, failure type, Delivery Group, and time period to view a graph containing more detailed information about the user connection failures across your site.
View trends for machine failures	From the Desktop OS Machine Failures tab or Server OS Machines tab, select the failure type, Delivery Group, and time period to view a graph containing more detailed information about the machine failures across your site.
View trends for logon performance	From the Logon Performance tab, select the Delivery Group and time period to view a graph containing more detailed information about the duration of user logon times across your site and whether the number of logons affects the performance. This view also shows the average duration of the logon

	phases, such as brokering duration, VM start time, and so on. This data is specifically for user logons and does not include users trying to reconnect from disconnected sessions.
View trends for load evaluation	From the Load Evaluator Index tab, view a graph containing more detailed information about the load that is distributed among Server OS machines. The filter options for this graph include the Delivery Group or Server OS machine in a Delivery Group, Server OS machine (available only if Server OS machine in a Delivery Group was selected), and range.
View hosted applications usage	The availability of this feature depends on your organization's license. From the Hosted Applications Usage tab, select the Delivery Group and time period to view a graph displaying peak concurrent usage and a table displaying application based usage. From the Application Based Usage table, you can choose a specific application to see details and a list of users who are using, or have used, the application.
View virtual machine usage	From the Machine Usage tab, select Desktop OS Machines or Server OS Machines to obtain real-time view of your VM usage, enabling you to quickly assess your site's capacity needs. Desktop OS availability — displays the current state of Desktop OS machines (VDIs) by availability for the entire site or specific Delivery Group. Server OS availability — displays the current state of Server OS machines by availability for the entire site or specific Delivery Group.
View network analysis data using HDX Insight	The availability of this feature depends on your organization's license and your administrator permissions. From the Network tab, monitor your network analysis, which provides a user, application, and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in your deployment.

The flag icons on the graph indicate significant events or actions for that specific time range. Hover the mouse over the flag and click to list events or actions.

Note: HDX connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.

Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

Monitor historical trends across a site - XenApp 7.6 and XenDesktop 7.6

The Trends view accesses historical trend information for sessions, connection failures, machine failures, logon performance, and load evaluation for each site. To locate this information, click from the Dashboard or Filters view, click Trends.

To change the default scope of each graph, apply a different filter to the data.

Action	Description
Export graph data	Select the tab containing the data to export. Click Export and select the file format: .PDF or .CSV.
View trends for sessions	From the Sessions tab, select the Delivery Group and time period to view more detailed information about the concurrent session count.
View trends for connection failures	From the Connection Failures tab, select the machine type, failure type, Delivery Group, and time period to view a graph containing more detailed information about the user connection failures across your site.
View trends for machine failures	From the Desktop OS Machine Failures tab or Server OS Machines tab, select the failure type, Delivery Group, and time period to view a graph containing more detailed information about the machine failures across your site.
View trends for logon performance	From the Logon Performance tab, select the Delivery Group and time period to view a graph containing more detailed information about the duration of user logon times across your site and whether the number of logons affects the performance. This view also shows the average duration of the logon phases, such as brokering duration, VM start time, and so on. This data is specifically for user logons and does not include users trying to reconnect from disconnected sessions.
View trends for load evaluation	From the Load Evaluator Index tab, view a graph containing more detailed information about the load that is distributed among Server OS machines. The filter options for this graph include the Delivery Group or Server OS machine in a Delivery Group, Server OS machine (available only if Server OS machine in a Delivery Group was selected), and range.
View hosted applications usage	The availability of this feature depends on your organization's license. From the Hosted Applications Usage tab, select the Delivery Group and time period to view a graph displaying peak concurrent usage and a table displaying application based usage. From the Application Based Usage table, you can choose a specific application to see details and a list of users who are using, or have used, the application.
View network analysis data using HDX Insight	The availability of this feature depends on your organization's license and your administrator permissions. From the Network tab, monitor your network analysis, which provides a user, application, and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in your deployment.

The flag icons on the graph indicate significant events or actions for that specific time range. Hover the mouse over the flag and click to list events or actions.

Note: HDX connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.
Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

Monitor hotfixes

To view the hotfixes installed on a specific machine VDA (physical or VM), choose the Machine Details view.

Control user machine power states

To control the state of the machines that you select in Director, use the Power Control options. These options are available for Desktop OS machines, but might not be available for Server OS machines.

Note: This functionality is not available for physical machines or machines using Remote PC Access.

Command	Function
Restart	Performs an orderly (soft) shutdown of the VM. and all running processes are halted individually before restarting the VM. For example, select machines that appear in Director as "failed to start," and use this command to restart them.
Force Restart	Restarts the VM without first performing any shut-down procedure. This command works in the same way as unplugging a physical server and then plugging it back in and turning it back on.
Shut Down	Performs an orderly (soft) shutdown of the VM; all running processes are halted individually.
Force Shutdown	Shuts down the VM without first performing any shut-down procedure. This command works in the same way as unplugging a physical server. It may not always shut down all running processes, and you risk losing data if you shut down a VM in this way.
Suspend	Suspends a running VM in its current state and stores that state in a file on the default storage repository. This option allows you to shut down the VM's host server and later, after rebooting it, resume the VM, returning it to its original running state.
Resume	Resumes a suspended VM and restores its original running state.
Start	Starts a VM when it is off (also called a cold start).

If power control actions fail, hover the mouse over the alert, and a pop-up message appears with details about the failure.

Prevent connections to machines

Use maintenance mode to prevent new connections temporarily while the appropriate administrator performs maintenance tasks on the image.

When you enable maintenance mode on machines, no new connections are allowed until you disable it. If users are currently logged on, maintenance mode takes effect as soon as all users are logged off. For users who do not log off, send a message informing them that machines will be shut down at a certain time, and use the power controls to force the machines to shut down.

1. Select the machine, such as from the User Details view, or a group of machines in the Filters view.
2. Select Maintenance Mode, and turn on the option.

If a user tries to connect to an assigned desktop while it is in maintenance mode, a message appears indicating that the desktop is currently unavailable. No new connections can be made until you disable maintenance mode.

Troubleshoot user issues

Oct 08, 2014

Use the Director's **Help Desk** view (**Activity Manager** page) to view information about the user:

- Check for details about the user's logon, connection, and applications.
- Shadow the user's machine.
- Troubleshoot the issue with the recommended actions in the following table, and, if needed, escalate the issue to the appropriate administrator.

Troubleshooting tips

User's issue	See these suggestions:
Logon takes a long time or fails intermittently or repeatedly	Diagnose user logon issues
Application is slow or won't respond	Resolve application failures
Connection failed	Restore desktop connections
Session is slow or not responding	Restore sessions
Video is slow or poor quality	Run HDX channel system reports

Note: To make sure that the machine is not in maintenance mode, from the User Details view, review the Machine Details panel.

Search tips

When you type the user's name in a Search field, Director searches for users in Active Directory for users across all sites configured to support Director.

When you type a multiuser machine name in a Search field, Director displays the Machine Details for the specified machine.

When you type an endpoint name in a Search field, Director uses the unauthenticated (anonymous) and authenticated sessions that are connected to a specific endpoint, which enables troubleshooting unauthenticated sessions. Ensure that endpoint names are unique to enable troubleshooting of unauthenticated sessions.

The search results also include users who are not currently using or assigned to a machine.

- Searches are not case-sensitive.
- Partial entries produce a list of possible matches.
- After you type a few letters of a two-part name (username, family name and first name, or display name), separated by a space, the results include matches for both strings. For example, if you type jo rob, the results might include strings such as “John Robertson” or Robert, Jones.

To return to the landing page, click the Director logo.

Upload troubleshooting information to Citrix Technical Support

Run Citrix Scout from a single Delivery Controller or VDA to capture key data points and Citrix Diagnosis Facility (CDF) traces to troubleshoot selected computers. After capturing this information, Scout securely uploads the data points to Citrix Technical Support. The Tools As a Service (TaaS) platform uses this information to reduce the time to resolve customer-reported issues.

Scout is installed with XenApp or XenDesktop components. Scout appears in the Windows Start Menu or Windows 8 or 8.1 Start Screen when you install or upgrade to XenDesktop 7.1, XenDesktop 7.5, or XenApp 7.5.

To start Scout, from the Start Menu or Start Screen, select Citrix > Citrix Scout.

For information on using and configuring Scout, and for frequently asked questions, see http://support.citrix.com/article/CTX130147.

The following video summarizes how to use Scout.

Shadow users

Oct 07, 2014

From Director, use the shadow user feature to view and work directly on a user's virtual machine or session. The user must be connected to the machine that you want to shadow. Verify this by checking the machine name listed in the user title bar.

1. In the User Details view, select the user session.
2. Activate shadowing for the selected user session:
   - For machine monitoring, in the Activity Manager view, click Shadow.
   - For session monitoring, in the User Details view, locate the Session Details panel and click Shadow.
3. After the connection initializes, a dialog box prompts you to open or save the `.msrcincident` file.
4. Open the incident file with the Remote Assistance Viewer, if not already selected by default. A confirmation prompt appears on the user device.
5. Instruct the user to click Yes to start the machine or session sharing.

For additional control, ask the user to share keyboard and mouse control.

Streamline Microsoft Internet Explorer browsers for shadowing

Configure your Microsoft Internet Explorer browser to automatically open the downloaded Microsoft Remote Assistance (.msra) file with the Remote Assistance client.

To do this, you must enable the Automatic prompting for file downloads setting in the Group Policy editor:

Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone > Automatic prompting for file downloads.

By default, this option is enabled for sites in the Local intranet zone. If the Director site is not in the Local intranet zone, consider manually adding the site to this zone.

Send messages to users

Jul 07, 2014

From Director, send a message to a user who is connected to one or more machines. For example, use this feature to send immediate notices about administrative actions such as impending desktop maintenance, machine log-offs and restarts, and profile resets.

1. In the Activity Manager view, select the user and click Details.
2. In the User Details view, locate the Session Details panel and click Send Message.
3. Type your message information in the Subject and Message fields, and click Send.

If the message is sent successfully, a confirmation message appears in Director. If the user's machine is connected, the message appears there.

If the message is not sent successfully, an error message appears in Director. Troubleshoot the problem according to the error message. When you have finished, type the subject and message text again and click Try again.

Diagnose user logon issues

Jul 07, 2014

Use these general steps:

1. From the User Details view, troubleshoot the logon state using the Logon Duration panel.
   - If the user is logging on, the view reflects the process of logging on.
   - If the user is currently logged on, the Logon Duration panel displays the time it took for the user to log on to the current session.
2. Ask the user to log off and then log on again so that you can observe the Logon Duration data. The panel typically updates after about 3 minutes, but it could take longer depending on the time taken for the logon to complete.
3. Examine the phases of the logon process:
   - **Brokering** — Time taken to decide which desktop to assign to the user.
   - **VM start** — Time taken to boot the desktop.
   - **HDX connection** — Time taken for HDX connection establishment, dependent on the network.
   - **GPOs** — Time taken to apply group policy objects.
   - **Login scripts** — Time taken for scripts.
   - **Profile load** — Time taken to load the user profile.
   - **Interactive session** — Time taken to establish an interactive user session.

   The total logon time is not an exact sum of these phases. For example, some phases occur in parallel, and in some phases, additional processing occurs that might result in a longer logon duration than the sum.

   Tip: To identify unusual or unexpected values in the graph, compare the amount of time taken in each phase of the current session with the average duration for this user for the last seven days, and the average duration for all users in this Delivery Group for the last seven days.

   Escalate as needed. For example, if the VM startup is slow, the issue could be in the hypervisor, so you can escalate it to the hypervisor administrator. Or, if the brokering time is slow, you can escalate the issue to the Site administrator to check the load balancing on the Delivery Controller.

Troubleshooting tips: Examine unusual differences, including:

- Missing (current) logon bars
- Major discrepancy between the current duration and this user's average duration. Causes could including:
  - A new application was installed.
  - An operating system update occurred.
  - Configuration changes were made.
- Major discrepancy between the user's logon numbers (current and average duration) and the Delivery Group average duration.

If needed, click Restart to observe the user's logon process to troubleshoot issues, such as VM Start or Brokering.

Resolve application failures

Jul 07, 2014

In the Activity Manager view, click the Applications tab. You can view all the applications on all machines to which this user has access, including local and hosted applications for the currently connected machine, and the current status of each.
Note: If the Applications tab is greyed out, contact an administrator with the permission to enable the tab.
The list includes only those applications that were launched within the session.

For Server OS machines and Desktop OS machines, applications are listed for each disconnected session. If the user is not connected, no applications are displayed.

Action	Description
End the application that is not responding.	Choose the application that is not responding and click End Application. Once the application is terminated, ask the user to launch it again.
End processes that are not responding.	If you have the required permission, click the Processes tab. Select a process that is related to the application or using a high amount of CPU resources or memory, and click End Process. However, if you do not have the required permission to terminate the process, attempting to end a process will fail.
Restart the user's machine.	For Desktop OS machines only, for the selected session, click Restart, Alternatively, from the Machine Details view, use the power controls to restart or shut down the machine. Instruct the user to log on again so that you can recheck the application. For Server OS machines, the restart option is not available. Instead, log off the user and let the user log on again.
Put the machine into maintenance mode.	If the machine's image needs maintenance, such as a patch or other updates, put the machine into maintenance mode and escalate the issue to the appropriate administrator. Click , and from the Machine Details view, click Details and turn on the maintenance mode option. Escalate to the appropriate administrator.

Restore desktop connections

Jul 07, 2014

From Director, check the user's connection status for the current machine in the user title bar.

If the desktop connection failed, the error that caused failure is displayed and can help you decide how to troubleshoot.

Action	Description
Ensure that the machine is not in maintenance mode.	On the User Details page, make sure maintenance mode is turned off.
Restart the user's machine.	Select the machine and click Restart. Use this option if the user's machine is unresponsive or unable to connect, such as when the machine is using an unusually high amount of CPU resources, which can make the CPU unusable.

Restore sessions

Jul 07, 2014

If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the server.

In the User Details view, troubleshoot session failures in the Session Details panel. You can view the details of the current session, indicated by the session ID.

Action	Description
End applications or processes that are not responding.	Click the Applications tab. Select any application that is not responding and click End Application. Similarly, select any corresponding process that is not responding and click End Process. Also, end processes that are consuming an unusually high amount of memory or CPU resources, which can make the CPU unusable.
Disconnect the Windows session.	Click Session Control and then select Disconnect. This option is available only for brokered Server OS machines. For non-brokered sessions, the option is disabled.
Log off the user from the session.	Click Session Control and then select Log Off.

To test the session, the user can attempt to log back onto it. You can also shadow the user to more closely monitor this session.

Note: If user devices are running Virtual Delivery Agents (VDAs) earlier than XenDesktop 7, Director cannot display complete information about the session; instead, it displays a message that the information is not available. These messages might appear in the User Details page and Activity Manager.

Run HDX channel system reports

Jul 07, 2014

In the User Details view, check the status of the HDX channels on the user's machine in the HDX panel. This panel is available only if the user machine is connected using HDX.
If a message appears indicating that the information is not currently available, wait for one minute for the page to refresh, or select the Refresh button. HDX data takes a little longer to update than other data.

Click an error or warning icon for more information.

Tip: You can view information about other channels in the same dialog box by clicking the left and right arrows in the left corner of the title bar.
HDX channel system reports are used mainly by Citrix Support to troubleshoot further.

1. In the HDX panel, click Download System Report.
2. You can view or save the .xml report file.
   - To view the .xml file, click Open. The .xml file appears in the same window as the Director application.
   - To save the .xml file, click Save. The Save As window appears, prompting you for a location on the Director machine to download the file to.

Reset a Personal vDisk

Jul 07, 2014

Caution: When you reset the disk, the settings revert back to their factory default values and all data on it is deleted, including applications. The profile data is retained unless you modified the Personal vDisk default (of redirecting profiles from the C: drive), or you are not using a third-party profile solution.

To reset, the machine with the Personal vDisk must be running; however, the user does not have to be logged on to it.

This option is available only for Desktop OS machines; it is disabled for Server OS machines.

1. From the Help Desk view, choose the targeted Desktop OS machine.
2. From this view or in the Personalization panel of the User Details view, click Reset Personal vDisk.
3. Click Reset. A message appears warning that the user will be logged off. After the user is logged off (if the user was logged on), the machine restarts.

If the reset is successful, the Personal vDisk status field value in the Personalization panel of the User Details view is Running. If the reset is unsuccessful, a red X to the right of the Running value appears. When you point to this X, information about the failure appears.

Reset a user profile

Apr 21, 2015

Caution: When a profile is reset, although the user's folders and files are saved and copied to the new profile, most user profile data are deleted (for example, the registry is reset and application settings might be deleted).

1. From Director, search for the user whose profile you want to reset and select this user's session.
2. Click **Reset Profile**.
3. Instruct the user to log off from all sessions.
4. Instruct the user to log on again. The folders and files that were saved from the user's profile are copied to the new profile.
   Important: If the user has profiles on multiple platforms (such as Windows 8 and Windows 7), instruct the user to log back on first to the same desktop or app that the user reported as a problem. This ensures that the correct profile is reset.
   If the profile is a Citrix user profile, the profile is already reset by the time the user's desktop appears. If the profile is a Microsoft roaming profile, the folder restoration might still be in progress for a brief time. The user must stay logged on until the restoration is complete.

Note: The preceding steps assume you are using XenDesktop (desktop VDA). If you are using XenApp (server VDA) you will need to be logged on to perform the profile reset. The user then needs to log off, and log back on to complete the profile reset.

If the profile is not successfully reset (for example, the user cannot successfully log back on to the machine or some of the files are missing), you must manually restore the original profile.

The folders (and their files) from the user's profile are saved and copied to the new profile. They are copied in the listed order:

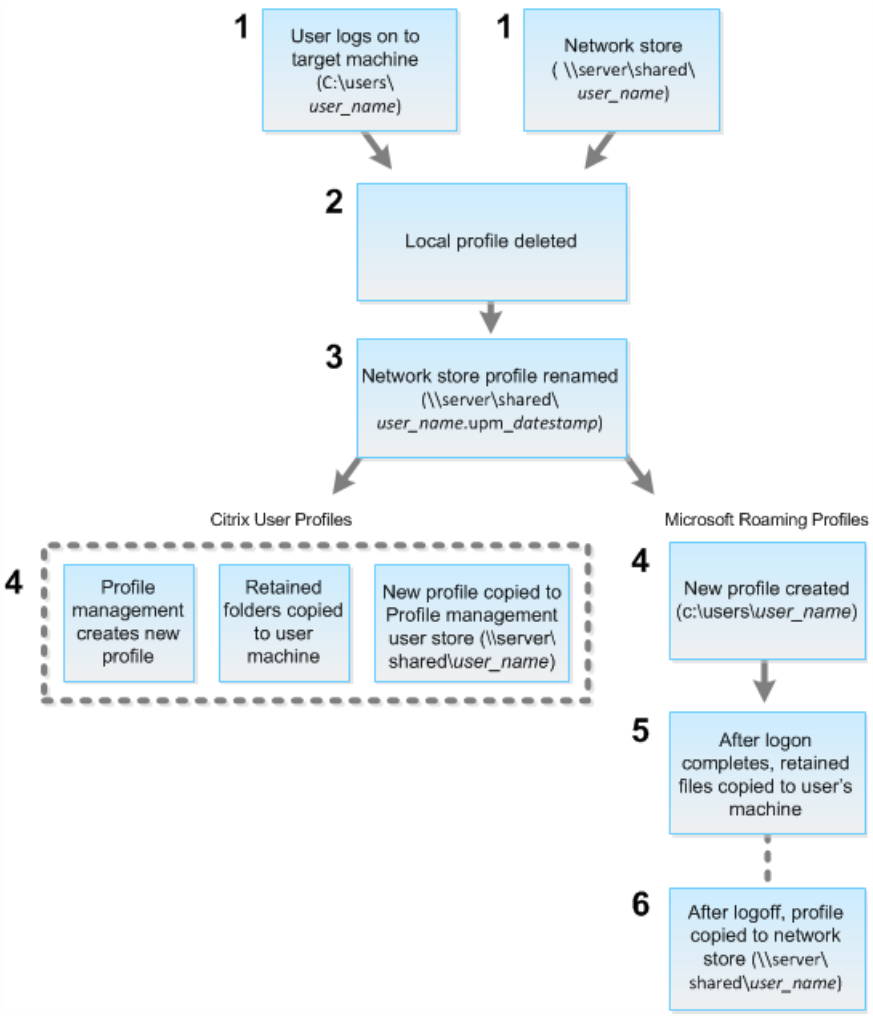
- Desktop
- Cookies
- Favorites
- Documents
- Pictures
- Music
- Videos

Note: In Windows 8 and later, cookies are not copied when profiles are reset.

How reset profiles are processed

Any Citrix user profile or Microsoft roaming profile can be reset. After the user logs off and you select the reset command (either in Director or using the PowerShell SDK), Director first identifies the user profile in use and issues an appropriate reset command. Director receives the information through Profile management, including information about the profile size, type, and logon timings.

The next time the user logs on, this diagram illustrates the processing that occurs.



1. The reset command issued by Director specifies the profile type. The Profile management service then attempts to reset a profile of that type and looks for the appropriate network share (user store). If the user is processed by Profile management, but receives a roaming profile command, it is rejected (or vice versa).
2. If a local profile is present, it is deleted.
3. The network profile is renamed.
4. The next action depends on whether the profile being reset is a Citrix user profile or a Microsoft roaming profile.
   - For Citrix user profiles, the new profile is created using the Profile management import rules, and the folders are copied back to the network profile, and the user can log on proceeds as normal. If a roaming profile is used for the reset, any registry settings in the roaming profile are preserved in the reset profile.
     Note: You can configure Profile management so that a template profile overrides the roaming profile, if required.
   - For Microsoft roaming profiles, a new profile is created by Windows, and when the user logs on, the folders are copied back to the user device. When the user logs off again, the new profile is copied to the network store.

To manually restore a profile after a failed reset

1. Instruct the user to log off from all sessions.
2. Delete the local profile if one exists.
3. Locate the archived folder on the network share that contains the date and time appended to the folder name, the folder with a .upm_datestamp extension.
4. Delete the current profile name; that is, the one without the upm_datestamp extension.
5. Rename the archived folder using the original profile name; that is, remove the date and time extension. You have returned the profile to its original, pre-reset state.

Session Recording - for XenApp 7.6 FP1, FP2, and LTSR

Apr 07, 2016

Session Recording allows you to record the on-screen activity of any user session hosted from a Server OS VDA machine, over any type of connection, subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback.

Session Recording uses flexible policies to trigger recordings of application sessions automatically. This enables IT to monitor and examine user activity of applications — such as financial operations and healthcare patient information systems — supporting internal controls for regulatory compliance and security monitoring. Similarly, Session Recording also aids in technical support by speeding problem identification and time-to-resolution.

Benefits

Enhanced security through logging and monitoring. Session Recording allows organizations to record on-screen user activity for applications that deal with sensitive information. This is especially critical in regulated industries such as health care and finance. Where personal information that must not be recorded is involved, policy controls allow selective recording.

Powerful activity monitoring. Session Recording captures and archives screen updates, including mouse activity and the visible output of keystrokes in secured video recordings to provide a record of activity for specific users, applications, and servers.

Session Recording is not designed or intended to contribute to the collection of evidence for legal proceedings. Citrix recommends that organizations using Session Recording use other techniques for evidence collection, such as conventional video records combined with traditional text-based eDiscovery tools.

Faster problem resolution. When users call with a problem that is hard to reproduce, help desk support staff can enable recording of user sessions. When the issue recurs, Session Recording provides a time-stamped visual record of the error, which can then be used for faster troubleshooting.

Get started with Session Recording

Feb 25, 2015

After you perform the following steps, you can begin recording and reviewing XenApp sessions.

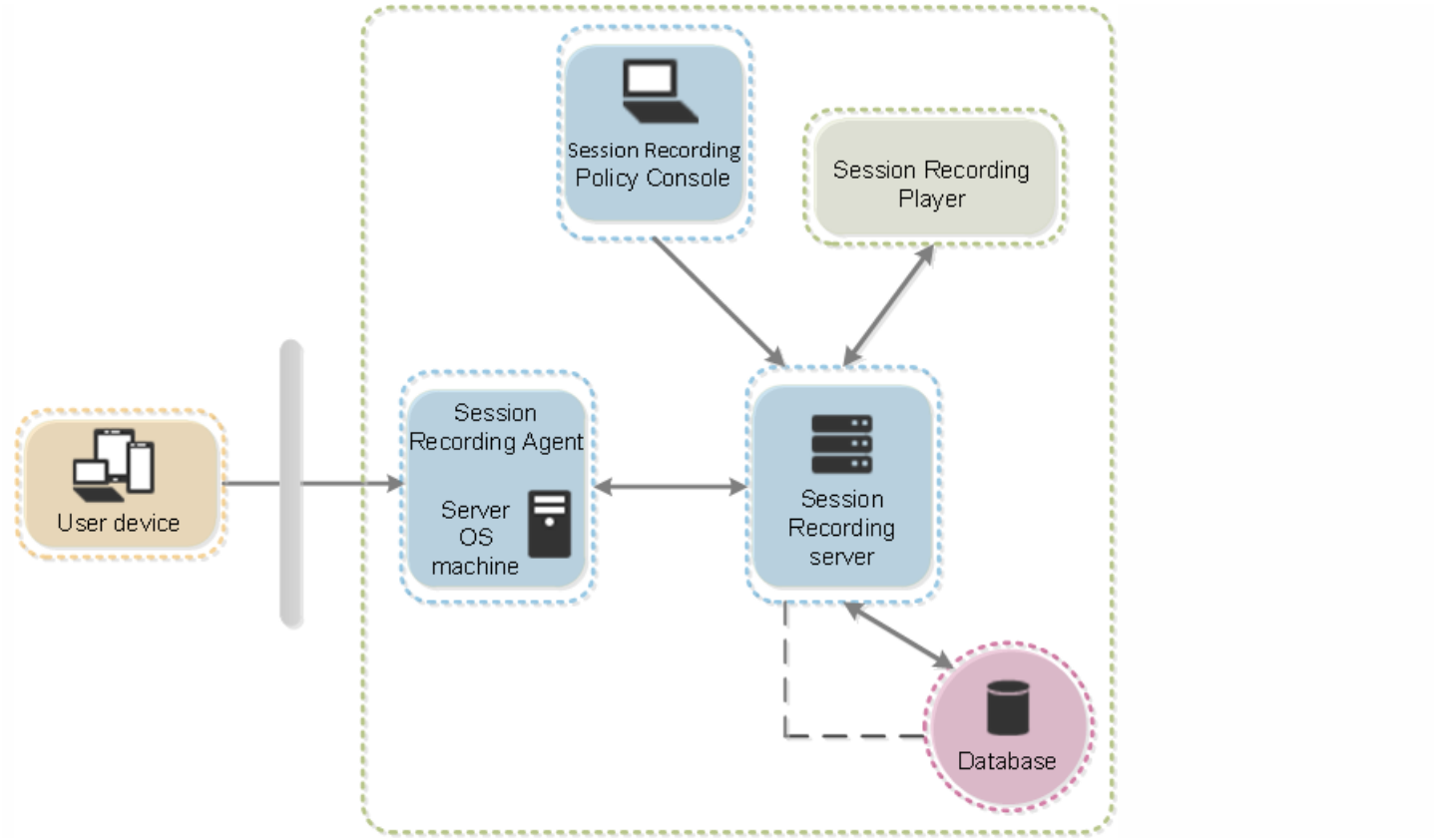
1. Become familiar with the Session Recording components.
2. Select the deployment scenario for your environment.
3. Verify the installation requirements.
4. Install Session Recording.
5. Configure the Session Recording components to permit recording and viewing of sessions.

Session Recording consists of five components:

- **Session Recording Agent.** A component installed on each Server OS machine to enable recording. It is responsible for recording session data.
- **Session Recording Server.** A server that hosts:
  - The Broker. An IIS 6.0+ hosted Web application that handles the search queries and file download requests from the Session Recording Player, handles policy administration requests from the Session Recording Policy Console, and evaluates recording policies for each XenApp session.
  - The Storage Manager. A Windows service that manages the recorded session files received from each Session Recording-enabled computer running XenApp.
- **Session Recording Player.** A user interface that users access from a workstation to play recorded XenApp session files.
- **Session Recording Database.** An SQL database for storing recorded session data.
- **Session Recording Policy Console.**A console used to create policies to specify which sessions are recorded.

This illustration shows the Session Recording components and their relationship with each other:

In the deployment example illustrated here, the Session Recording Agent, Session Recording Server, Session Recording Database, Session Recording Policy Console, and Session Recording Player all reside behind a security firewall. The Session Recording Agent is installed on a Server OS machine. A second server hosts the Session Recording Policy Console, a third server acts as the Session Recording Server, and a fourth server hosts the Session Recording Database. The Session Recording Player is installed on a workstation. A client device outside the firewall communicates with the Server OS machine on which the Session Recording Agent is installed. Inside the firewall, the Session Recording Agent, Session Recording Policy Console, Session Recording Player, and Session Recording Database all communicate with the Session Recording Server.



Plan your deployment

Feb 25, 2015

Depending upon your environment, you can deploy the Session Recording components in different scenarios.

A Session Recording deployment does not have to be limited to a single site. With the exception of the Session Recording Agent, all components are independent of the server site. For example, you can configure multiple sites to use a single Session Recording Server.

Alternatively, if you have a large site with many agents and plan to record many graphically intense applications (for example, AutoCAD applications), or you have many sessions to record, a Session Recording Server can experience a high performance demand. To alleviate performance issues, you can install multiple Session Recording Servers on different computers and point the Session Recording Agents to the different computers. Keep in mind that an agent can point to only one server at a time.

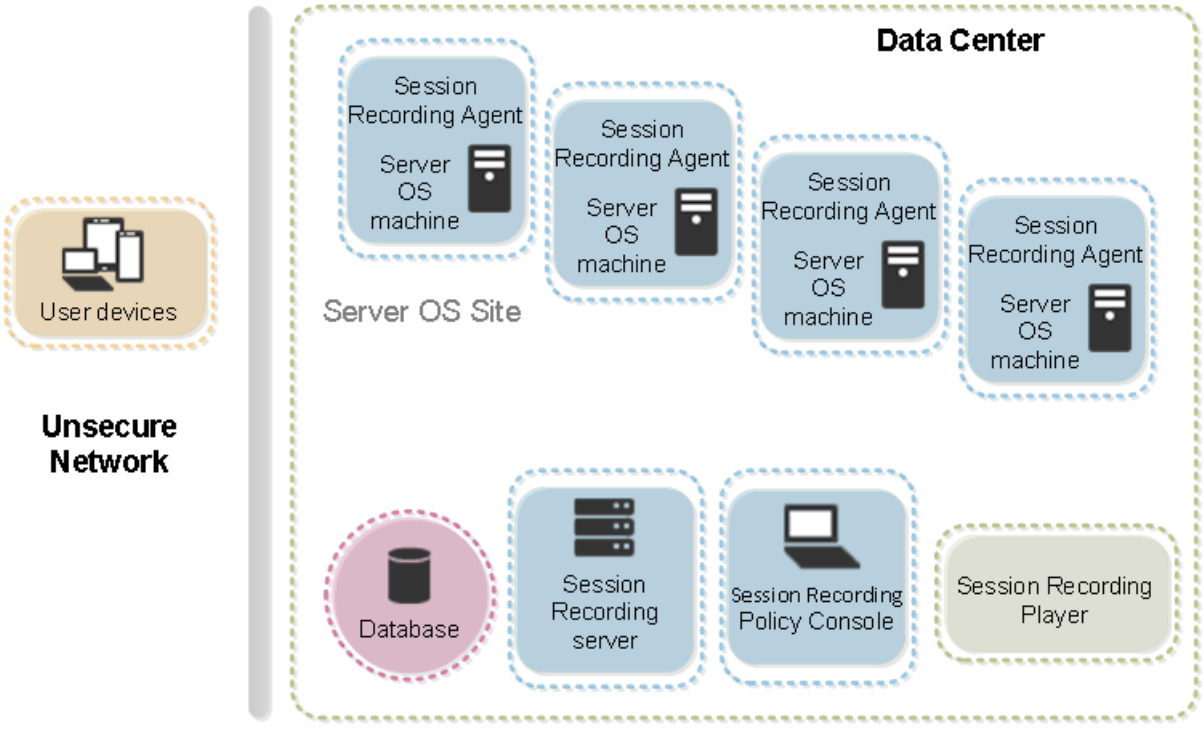
Suggested deployment scenarios

These are the two suggested configurations for a Session Recording deployment:

- Deploy the Session Recording Agent on single Server OS machine.
- Deploy the Session Recording Agent on multiple Server OS machines on a site.

Server site deployment

Use this type of deployment for recording sessions for one or more sites. The Session Recording Agent is installed on each Server OS machine in a site. The site resides in a data center behind a security firewall. The Session Recording Administration components (Session Recording Database, Session Recording Server, Session Recording Policy Console) are installed on other servers and the Session Recording Player is installed on a workstation, all behind the firewall but not in the data center. Outside the firewall, in an unsecured network environment, are XenApp clients, such as a workstation, mobile devices, and a laptop computer.



Security recommendations

Nov 30, 2016

Session Recording is designed to be deployed within a secure network and accessed by administrators, and as such, is secure. Out-of-the-box deployment is designed to be simple and security features such as digital signing and encryption can be configured optionally.

Communication between Session Recording components is achieved through Internet Information Services (IIS) and Microsoft Message Queuing (MSMQ). IIS provides the web services communication link between each Session Recording component. MSMQ provides a reliable data transport mechanism for sending recorded session data from the Session Recording Agent to the Session Recording Server.

Consider these security recommendations when planning your deployment:

- Ensure servers running Session Recording components are physically secure. If possible, lock these computers in a secure room to which only authorized personnel can gain direct access.
- Isolate servers running Session Recording components on a separate subnet or domain.
- Protect the recorded session data from users accessing other servers by installing a firewall between the Session Recording Server and other servers.
- Keep the Session Recording Admin Server and SQL database up to date with the latest security updates from Microsoft.
- Restrict nonadministrators from logging on to the administration machine.
- Strictly limit who is authorized to make recording policy changes and view recorded sessions.
- Install digital certificates, use the Session Recording file signing feature, and set up SSL communications in IIS.
- Set up MSMQ to use HTTPS as its transport by setting the MSMQ protocol listed in the Session Recording Agent Properties dialog box to HTTPS. For more information, see Troubleshoot MSMQ.
- Use TLS 1.0 and disable SSLv2, SSLv3, and RC4 cipher on the Session Recording Server and Session Recording Database. For more information, see the Microsoft articles http://support.microsoft.com/default.aspx?scid=kb;en-us;187498 and http://support.microsoft.com/kb/245030/en-us.
- Use playback protection. Playback protection is a Session Recording feature that encrypts recorded files before they are downloaded to the Session Recording Player. By default, this option is enabled and is in the Session Recording Server Properties.
- Follow NSIT guidance for cryptographic key lengths and cryptographic algorithms.

For information about configuring Session Recording features, see http://support.citrix.com/article/CTX200868.

-

Install certificates

On the computer on which the Session Recording Server is installed, the IIS Web server sends its server certificate to the client when establishing an SSL connection from the Session Recording Agent, Session Recording Player, or Session Recording Policy Console. When receiving a server certificate, the Session Recording Agent, Session Recording Player, or Policy Console determines which Certificate Authority (CA) issued the certificate and if the CA is trusted by the client. If the CA is not trusted, the certificate is declined and an error is logged in the Application Event log for the Session Recording Agent or an error message appears to the user in the Session Recording Player or Policy Console.

A server certificate is installed by gathering information about the server and requesting a CA to issue a certificate for that server. You must specify the correct information when requesting a server certificate and ensure the server name is specified

correctly. If the fully qualified domain name (FQDN) is used for connecting clients (Session Recording Agent, Session Recording Player, and Policy Console) the certificate information specified to the CA must use the FQDN of the server rather than the NetBIOS name. If you specify NetBIOS names, do not specify the FQDN when requesting a server certificate. Install the server certificate into the local server's certificate store. Install the issuing CA certificate on each connecting client.

Your organization may have a private CA that issues server certificates that you can use with Session Recording. If you are using a private CA, ensure each client device has the issuing CA certificate installed. Refer to Microsoft documentation about using certificates and certificate authorities. Alternatively, some companies and organizations currently act as CAs, including VeriSign, Baltimore, Entrust, and their respective affiliates.

All certificates have an expiration date defined by the CA. To find the expiration date, check the properties of the certificate. Ensure certificates are renewed before the expiration date to prevent any errors occurring in Session Recording.

The Session Recording installation is configured to use HTTPS by default and requires that you configure the default Web site with a server certificate issued from a CA. If you need instructions for installing server certificates in IIS, consult your IIS documentation.

Scalability considerations

Apr 23, 2015

Installing and running Session Recording requires few additional resources beyond what is necessary to run XenApp. However, if you plan to use Session Recording to record a large number of sessions or if the sessions you plan to record will result in large session files (for example, graphically intense applications), consider the performance of your system when planning your Session Recording deployment.

For more information about building a highly scalable Session Recording system, see http://support.citrix.com/article/CTX200869.

In this article:

Hardware recommendations

Consider how much data you will be sending to each Session Recording Server and how quickly the servers can process and store this data. The rate at which your system can store incoming data must be higher than the data input rate.

To estimate your data input rate, multiply the number of sessions recorded by the average size of each recorded session and divide by the period of time for which you are recording sessions. For example, you might record 5,000 Microsoft Outlook sessions of 20MB each over an 8-hour work day. In this case, the data input rate is approximately 3.5MBps. (5,000 sessions times 20MB divided by 8 hours, divided by 3,600 seconds per hour.)

You can improve performance by optimizing the performance of a single Session Recording Server or by installing multiple Session Recording Servers on different computers.

Disk and storage hardware

Disk and storage hardware are the most important factors to consider when planning a Session Recording deployment. The write performance of your storage solution is especially important. The faster data can be written to disk, the higher the performance of the system overall.

Storage solutions suitable for use with Session Recording include a set of local disks controlled as RAID arrays by a local disk controller or by an attached Storage Area Network (SAN).

Note: Session Recording should not be used with Network-Attached Storage (NAS), due to performance and security problems associated with writing recording data to a network drive.
For a local drive set up, a disk controller with built-in cache memory enhances performance. A caching disk controller must have a battery backup facility to ensure data integrity in case of a power failure.

Network capacity

A 100Mbps network link is suitable for connecting a Session Recording Server. A gigabit Ethernet connection may improve performance, but does not result in 10 times greater performance than a 100Mbps link.

Ensure that network switches used by Session Recording are not shared with third-party applications that may compete for available network bandwidth. Ideally, network switches are dedicated for use with the Session Recording Server.

Computer processing capacity

Consider the following specification for the computer on which a Session Recording Server is installed:

- A dual CPU or dual-core CPU is recommended
- 2GB to 4GB of RAM is recommended

Exceeding these specifications does not significantly improve performance.

Deploy multiple Session Recording servers

If a single Session Recording Server does not meet your performance needs, you can install more Session Recording Servers on different machines. In this type of deployment, each Session Recording Server has its own dedicated storage, network switches, and database. To distribute the load, point the Session Recording Agents in your deployment to different Session Recording Servers.

Database scalability

The Session Recording Database requires Microsoft SQL Server 2014, Microsoft SQL Server 2012, or Microsoft SQL Server 2008 R2. The volume of data sent to the database is very small because the database stores only metadata about the recorded sessions. The files of the recorded sessions themselves are written to a separate disk. Typically, each recorded session requires only about 1KB of space in the database, unless the Session Recording Event API is used to insert searchable events into the session.

The Express Editions of Microsoft SQL Server 2014, Microsoft SQL Server 2012, and Microsoft SQL Server 2008 R2 impose a database size limitation of 10GB. At 1KB per recording session, the database can catalog about four million sessions. Other editions of Microsoft SQL Server have no database size restrictions and are limited only by available disk space. As the number of sessions in the database increases, performance of the database and speed of searches diminishes only negligibly.

If you are not making customizations through the Session Recording Event API, each recorded session generates four database transactions: two when recording starts, one when the user logs onto the session being recorded, and one when recording ends. If you used the Session Recording Event API to customize sessions, each searchable event recorded generates one transaction. Because even the most basic database deployment can handle hundreds of transactions per second, the processing load on the database is unlikely to be stressed. The impact is light enough that the Session Recording Database can run on the same SQL Server as other databases, including the XenApp or XenDesktop data store database.

If your Session Recording deployment requires many millions of recorded sessions to be cataloged in the database, follow Microsoft guidelines for SQL Server scalability.

Important deployment notes

Mar 24, 2015

- To enable Session Recording components to communicate with each other, ensure you install them in the same domain or across trusted domains that have a transitive trust relationship. The system cannot be installed into a workgroup or across domains that have an external trust relationship.
- Session Recording does not support the clustering of two or more Session Recording Servers in a deployment.
- Due to its intense graphical nature and memory usage when playing back large recordings, Citrix does not recommend installing the Session Recording Player as a published application.
- The Session Recording installation is configured for SSL/HTTPS communication. Ensure that you install a certificate on the Session Recording Server and that the root certificate authority (CA) is trusted on the Session Recording components.
- If you install the Session Recording Database on a stand-alone server running SQL Server 2014 Express Edition, SQL Server 2012 Express Edition, or SQL Server 2008 R2 Express Edition, the server must have TCP/IP protocol enabled and SQL Server Browser service running. These settings are disabled by default, but they must be enabled for the Session Recording Server to communicate with the database. See the Microsoft documentation for information about enabling these settings.
- Consider the effects of session sharing when planning your Session Recording deployment. Session sharing for published applications can conflict with Session Recording recording policy rules for published applications. Session Recording matches the active policy with the first published application that a user opens. After the user opens the first application, any subsequent applications opened during the same session continue to follow the policy that is in force for the first application. For example, if a policy states that only Microsoft Outlook should be recorded, the recording commences when the user opens Outlook. However, if the user opens a published Microsoft Word second (while Outlook is running), Word also is recorded. Conversely, if the active policy does not specify that Word should be recorded, and the user launches Word before Outlook (which should be recorded, according to the policy), Outlook is not recorded.

Install Session Recording

Feb 07, 2017

This article contains installation instructions for XenApp 7.6 Feature Pack 2 and LTSR, and for Feature Pack 1 in separate sections.

XenApp 7.6 Feature Pack 2 and LTSR

Pre-Installation Checklist

Before you start the installation, ensure that you completed this list:

✓	Step
	Install the prerequisites before starting the installation. See System Requirements.
	Select the machines on which to install each Session Recording component and ensure that each computer meets the hardware and software requirements for the component or components to be installed on it.
	Download the Session Recording zip file from the LTSR download page.
	If you use the SSL protocol for communication between the Session Recording components, install the correct certificates in your environment. See Install certificates.
	Install any hotfixes required for the Session Recording components. The hotfixes are available from the Citrix Support.
	Configure Director to create and activate Session Recording policies.

Notes:

- Citrix recommends dividing the published applications into separate delivery groups based on the recording policies because session sharing for published applications can conflict with active policies if they are in the same delivery group. Session Recording matches the active policy with the first published application that a user opens.
- If you are planning to use Machine Creation Services (MCS) or Provisioning Services with XenApp, prepare the server for a unique QMId. See the description in Known issues. Failure to do this step might result in lost recording data.
- SQL server requires that TCP/IP is enabled, the SQL Server Browser service is running, and Windows Authentication.
- If you want to use HTTPS, configure server certificates for SSL/HTTPS.

Session Recording installation files

You need the following installation files from the Citrix download page:

- Session Recording Administration files
  - Broker_PowerShellSnapIn_x64.msi
  - SessionRecordingAdministrationx64.msi

- Session Recording Agent files
  - SessionRecordingAgentx64.msi
- Session Recording Player files
  - SessionRecordingPlayer.msi

Install Session Recording Administration components

The Session Recording Administration components are the Session Recording Database, Session Recording Server, and the Session Recording Policy Console. You can choose which of these components to install on a server.

Before installing the Session Recording Administration components, ensure you have all the prerequisites installed.
See Session Recording Administration components.

To improve security, you can remove these permissions after installing the database.

1. Run the **Broker_PowerShellSnapIn_x64.msi** and follow the instructions to complete the installation.
2. Start the Windows command prompt as Administrator, and then run this command:

   msiexec /i SessionRecordingAdministrationx64.msi

   or double click the .msi file.
3. On the installation UI, select Next and accept the license agreement.
4. On the Session Recording Administration Setup screen, select the Session Recording Administration components you want to install.

Install the Session Recording Database

Before installing the Session Recording Database, ensure you have all the prerequisites installed. See Session Recording Administration components.

1. On the Database Configuration page:
   - If you are installing all the Administration components on the same server, type **localhost** in the Session Recording Server Name field.
   - If you are installing the Session Recording Server and the Session Recording Database on different servers, type the name of the computer hosting the Session Recording Server in the following format: domain\machine-name. The Session Recording Server name is the user account for accessing the database.

If the database instance is not a named instance as you configured when you setup the instance, you can use only the machine name of the SQL Server. If you have named the instance, use machine-name\instance-name as the database instance name. To determine the server instance name you are using, run **select @@servername** on the SQL Server and the return value is the exact database instance name.
Click **Test** to test the connection to the SQL server. Make sure the current user has the public SQL Server role permission; otherwise the test fails for permission limitation. Then click **Next** to continue the installation.

2. Follow the instructions to complete the installation. During the installation, if current user is not the database administrator, a dialog box displays requiring the credentials of a database administrator with **sysadmin** server role permission. Enter the correct credentials and click **OK** to continue the installation. The installation creates the new Session Recording Database and adds the machine account of the Session Recording Server as **db-owner**.

Install the Session Recording Server

Before installing the Session Recording Server, ensure you have all the prerequisites installed. See Session Recording Administration components.

1. Enter the name of your SQL server in the Database Instance Name text box. If you are using a named instance, enter machine-name\instance-name; otherwise enter a machine-name only.
2. Click Test to test the connection to the SQL server. Make sure the current user has the public SQL Server role permission; otherwise the test fails for permission limitation. Then click **Next** to continue the installation and follow the instructions to complete the installation.
3. At the end of the installation wizard, you can choose to participate in the Citrix Customer Experience Improvement Program. When you join this program, anonymous statistics and usage information is sent to Citrix; for more information, see About the Citrix Customer Experience Improvement Program (CEIP).

Install the Session Recording Agent

The Session Recording Agent must be installed on the Server OS VDA machine on which you want to record sessions.

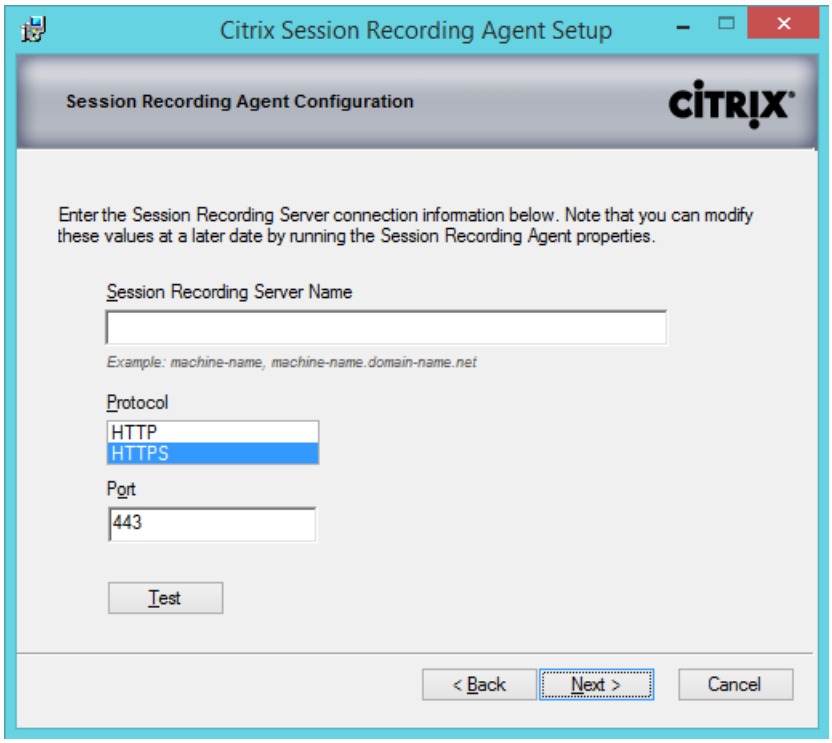
1. Use the Server Manager to install .NET Framework 3.5 and Microsoft Message Queuing (MSMQ) with HTTP support on

the XenApp 7.6 Server OS VDA.

2. Start the Windows command prompt as Administrator, and then run this command:

   msiexec /i SessionRecordingAgentx64.msi

   or double click the .msi file.
3. On the installation UI, select **Next** and accept the license agreement.
4. In the Session Recording Agent Configuration page, enter the name of the computer where you installed the Session Recording Server and the protocol and port information for the connection to the Session Recording Server.



The Session Recording default installation uses HTTPS/SSL to secure communications. If SSL is not configured, use HTTP. To do so, deselect SSL in the IIS Management Console by navigating to the Session Recording Broker site. Open the SSL settings and uncheck the Require SSL box.

5. For Feature Pack 2: If you want to use the Rollover feature, install Update ICATS760WX64010 (http://support.citrix.com/article/CTX142037). For LTSR: The Rollover feature is included in the LTSR version of the VDA (7.6.300). So, if your VDA is at LTSR level, the feature is available to you without further action.

6. Follow the instructions to complete the installation.

Install Session Recording Player

Install the Session Recording Player on the Session Recording Server or one or more workstations in the domain for users who view session recordings.

- Run the **SessionRecordingPlayer.msi** and follow the instructions to complete the installation.

Upgrade Session Recording

To upgrade Session Recording from XenApp 7.6 Feature Pack 1 or 2, run the installer on the machine where you installed corresponding Session Recording features.

Follow the instructions to finish the upgrade installation. You do not need to provide any information during the upgrade process.

XenApp 7.6 Feature Pack 1

Pre-Installation Checklist
Before you start the installation, ensure that you completed this list:

	**Step**
	Install the prerequisites before starting the installation. See System Requirements.
	Select the machines on which to install each Session Recording component and ensure that each computer meets the hardware and software requirements for the component or components to be installed on it.
	Download the Session Recording zip file from the Citrix download page under **XenApp > Components**.
	If you use the SSL protocol for communication between the Session Recording components, install the correct certificates in your environment. See Install certificates.
	Install any hotfixes required for the Session Recording components. The hotfixes are available from the Citrix Support.
	Configure Director to create and activate Session Recording policies.

Notes:

- Citrix recommends dividing the published applications into separate delivery groups based on the recording policies because session sharing for published applications can conflict with active policies if they are in the same delivery group. Session Recording matches the active policy with the first published application that a user opens.
- If you are planning to use Machine Creation Services (MCS) or Provisioning Services with XenApp, prepare the server for a unique QMId. See the description in Known issues. Failure to do this step might result in lost recording data.
- SQL server requires that TCP/IP is enabled, the SQL Server Browser service is running, and Windows Authentication.
- If you want to use HTTPS, configure server certificates for SSL/HTTPS.

Session Recording installation files

You need the following installation files from the Citrix download page:

- Session Recording Administration files
  - Broker_PowerShellSnapIn_x64.msi
  - SessionRecordingAdministrationx64.msi
- Session Recording Agent files
  - SessionRecordingAgentx64.msi

- Session Recording Player files
  - SessionRecordingPlayer.msi

Install Session Recording Administration components

The Session Recording Administration components are the Session Recording Database, Session Recording Server, and the Session Recording Policy Console. You can choose which of these components to install on a server.

Before installing the Session Recording Administration components, ensure you have all the prerequisites installed.
See Session Recording Administration components.

When installing the Session Recording Database on a local SQL Server, you must have NT AUTHORITY\SYSTEM as the login with the sysadmin SQL Server role permissions.

When installing the Session Recording Database on a remote SQL Server, you must have the machine account that is running the installer as the login with the sysadmin SQL Server role permissions.

To improve security, you can remove these permissions after installing the database.

1. Run the Broker_PowerShellSnapIn_x64.msi and follow the instructions to complete the installation.
2. Start the Windows command prompt as Administrator, and then run this command:

   msiexec /i SessionRecordingAdministrationx64.msi

   or double click the .msi file.
3. On the installation UI, select **Next** and accept the license agreement.
4. On the Session Recording Administration Setup screen, select the Session Recording Administration components you want to install.

Install the Session Recording Database

Before installing the Session Recording Database, ensure you have all the prerequisites installed. See Session Recording Administration components.

1. On the Database Configuration page:

- If you are installing all the Administration components on the same server, type **localhost** in the Session Recording Server Namefield.
- If you are installing the Session Recording Server and the Session Recording Database on different servers, type the name of the computer hosting the Session Recording Server in the following format: *domain**machine-name*. The Session Recording Server name is the user account for accessing the database.

If the database instance is not a named instance as you configured when you setup the instance, you can use only the machine name of the SQL Server. If you have named the instance, use m*achine-name\instance-name* as the database instance name. To determine the server instance name you are using, **run select @@servername** on the SQL Server and the return value is the exact database instance name.

2. Follow the instructions to complete the installation. The installation creates the new Session Recording Database and adds the machine account of the Session Recording Server as **db-owner**.

Install the Session Recording Server

Before installing the Session Recording Server, ensure you have all the prerequisites installed. See Session Recording Administration components.

- Enter the name of your SQL server in the Database Instance Name text box. If you are using a named instance, enter machine-name\instance-name; otherwise enter a machine-name only.

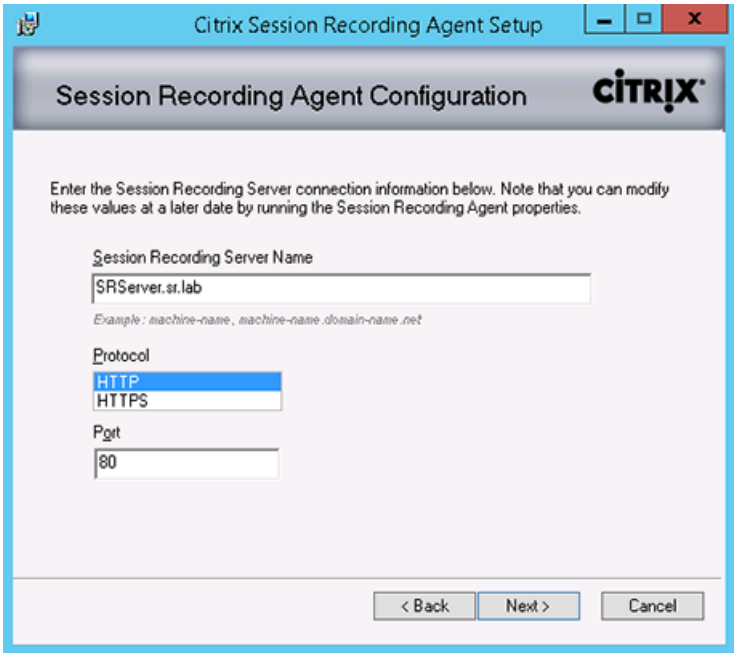
Install the Session Recording Agent

The Session Recording Agent must be installed on the Server OS VDA machine on which you want to record sessions.

1. Use the Server Manager to install .NET Framework 3.5 and Microsoft Message Queuing (MSMQ) with HTTP support on the XenApp 7.6 Server OS VDA.
2. Start the Windows command prompt as Administrator, and then run this command:

   msiexec /i SessionRecordingAgentx64.msi

   or double click the .msi file.
3. On the installation UI, select Next and accept the license agreement.
4. In the Session Recording Agent Configuration page, enter the name of the computer where you installed the Session Recording Server and the protocol and port information for the connection to the Session Recording Server.



The Session Recording default installation uses HTTPS/SSL to secure communications. If SSL is not configured, use HTTP. To do so, deselect SSL in the IIS Management Console by navigating to the Session Recording Broker site. Open the SSL settings and uncheck the Require SSL box.

5. If you want to use the Rollover feature, ensure that you install this hotfix: http://support.citrix.com/article/CTX142037.

6. Follow the instructions to complete the installation.

Install Session Recording Player

Install the Session Recording Player on the Session Recording Server or one or more workstations in the domain for users who view session recordings.

- Run the SessionRecordingPlayer.msi and follow the instructions to complete the installation.

Uninstall Session Recording

To remove Session Recording components from a server or workstation, use the uninstall or remove programs capability available through the Windows Control Panel. To remove the Session Recording Database, you must have the same sysadmin SQL server role permissions as when you installed it.

Configure Director to use the Session Recording Server

You can use the Director console to create and activate Session Recording policies.

1. For an https connection, install the certificate to trust the Session Recording Server in the Trusted Root Certificates of the Director server.
2. To configure the Director server to use the Session Recording Server, run this command: `C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording`
3. Enter the IP/FQDN of the Session Recording Server, the port number and connection type (http/https) from the Session Recording Agent to Session Recording Broker on Director server.

Automating installations

Feb 03, 2015

To install Session Recording Agent on multiple servers, write a script that uses silent installation.

The following command line installs the Session Recording Agent and creates a log file to capture the install information.

```
msiexec /i  SessionRecordingAgentx64.msi sessionrecordingservername=yourservername
sessionrecordingbrokerprotoco=yourbrokerprotocol sessionrecordingbrokerport=yourbrokerport
/l*v yourinstallationlog /q
```

where:

yourservername is the NetBIOS name or FQDN of the computer hosting the Session Recording Server. If not specified, this value defaults to localhost.

yourbrokerprotocol is either HTTP or HTTPS, and represents the protocol that Session Recording Agent uses to communicate with Session Recording Broker; this value defaults to HTTPS if not specified.

yourbrokerport is an integer representing the port Session Recording Agent uses to communicate with Session Recording Broker. If not specified, this value defaults to zero, which directs Session Recording Agent to use the default port number for the selected protocol: 80 for HTTP or 443 for HTTPS.

/l*v specifies verbose mode logging

yourinstallationlog is the location of the setup log file created.

/q specifies quiet mode.

Configure Session Recording to play and record sessions

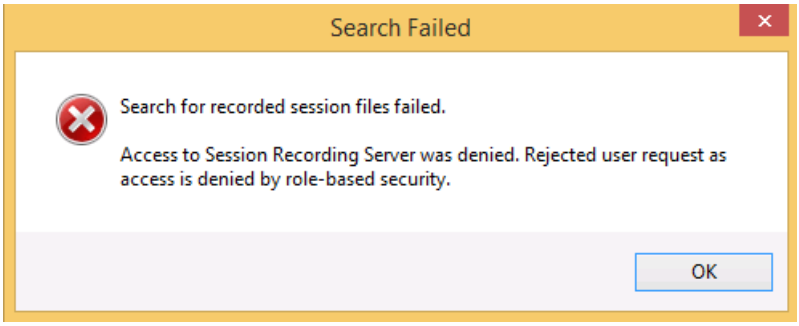
Sep 02, 2015

After you install the Session Recording components, perform these steps to configure Session Recording to record XenApp sessions and allow users to view them:

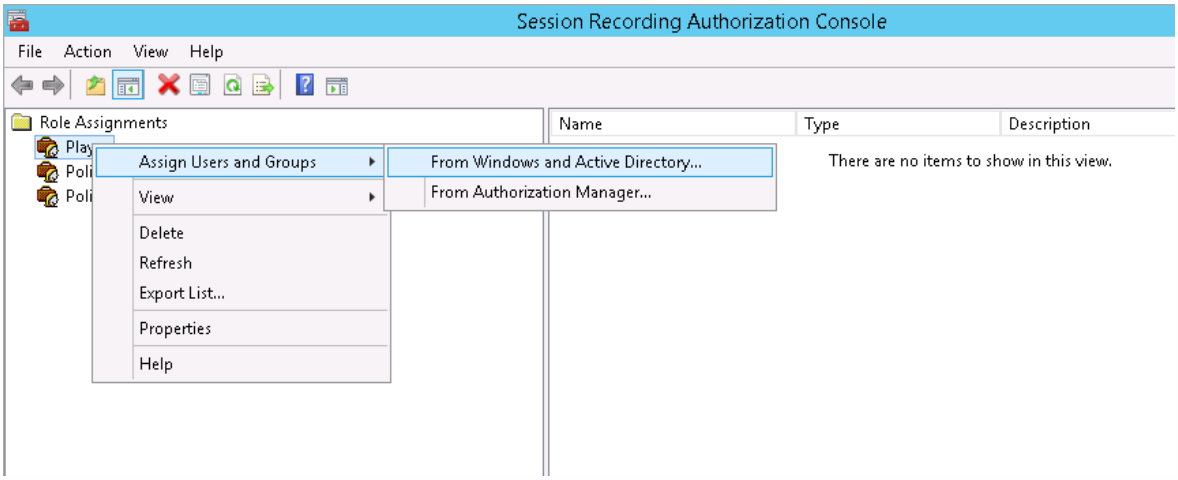
- Authorize users to play recordings
- Authorize users to administer recording policies
- Change the active recording policy to one that records sessions
- Configure Session Recording Player to connect to the Session Recording Server

Authorize users to play recorded sessions

When you install Session Recording, no users have permission to play recorded sessions. You must assign permission to each user, including the administrator. A user without permission to play recorded sessions receives the following error message when trying to play a recorded session:



1. Log on as administrator to the computer hosting the Session Recording Server.
2. Start the Session Recording Authorization Console.
3. In the Session Recording Authorization Console, select Player.
4. Add the users and groups you want to authorize to view recorded sessions and they will populate the right pane.



Authorize users to administer recording policies

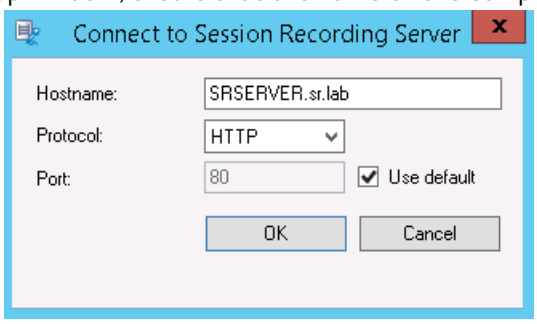
When you install Session Recording, domain administrators grant permission to control the recordng policies by default. You can change the authorization setting.

1. Log on as administrator to the machine hosting the Session Recording Server.
2. Start the Session Recording Authorization Console and select PolicyAdministrators.
3. Add the users and groups who can administer recording policies.

Set the active recording policy to record sessions

The active recording policy specifies session recording behavior on all Server OS VDAs that have Session Recording Agent installed and connected to the Session Recording Server. When you install Session Recording, the active recording policy is Do not record. Sessions cannot be recorded until you change the active recording policy.

1. Log on as an authorized Policy Administrator to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the computer hosting the Session Recording Server, protocol, and port are correct.



4. In the Session Recording Policy Console, expand Recording Policies. This displays the recording policies available when you install Session Recording, with a check mark indicating which policy is active:
   - Do not record. This is the default policy. If you do not specify another policy, no sessions are recorded.
   - Record everyone with notification. If you choose this policy, all sessions are recorded. A pop-up window appears notifying the user that recording is occurring.
   - Record everyone without notification. If you choose this policy, all sessions are recorded. A pop-up window does not appear notifying the user that recording is occurring.
5. Select the policy you want to make the active policy.
6. From the menu bar, choose Action > Activate Policy.

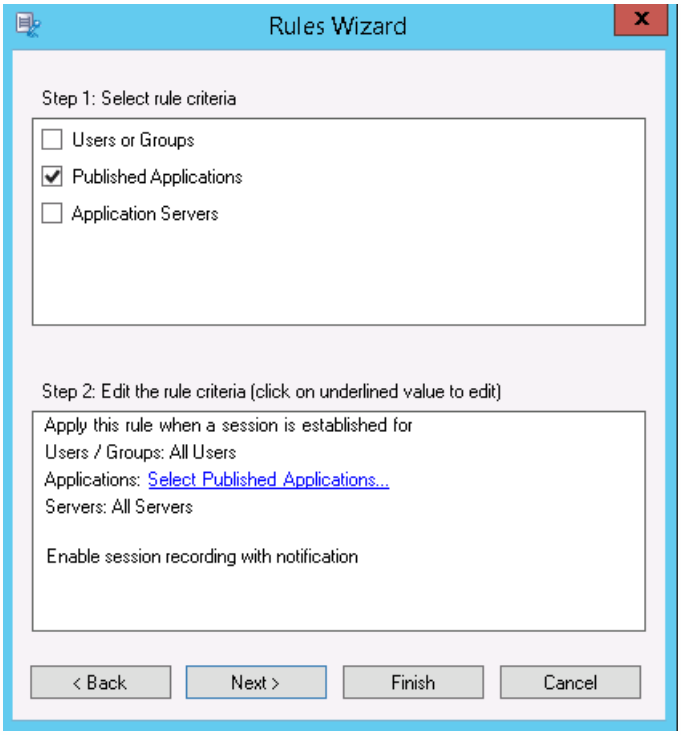
Note: Session Recording allows you to create your own recording policy. When you create recording policies, they appear in the Recording Policies folder within the Session Recording Policy Console.

Configure custom policies

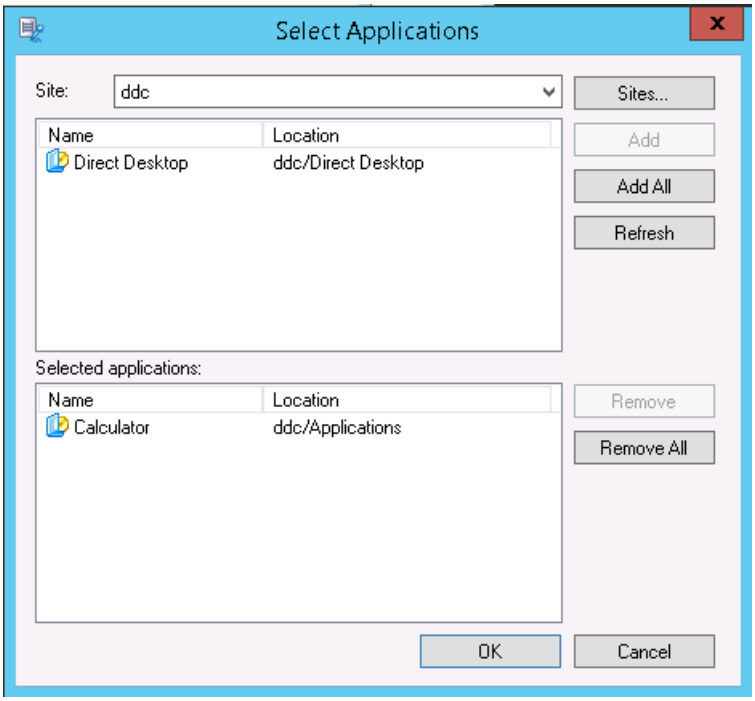
The generic recording policy might not fit your requirements. You can configure policies based on users, VDA servers, and applications.

Important: A policy can contain many rules, but there can be only one active policy running at a time.

1. Log on as an authorized Policy Administrator to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console and select Recording Policies > Add New Policy.
3. Right click New policy and select Add New Rule.
4. In the Rules wizard, select Enable Session Recording with notification , and then click Next.
5. Check the box Published Applications, and then click the hyperlink for Select Published Applications.



6. On the Select Applications screen, click Sites and Add.
7. Enter the server name of a XenApp 7.6 FP1 Delivery Controller.
8. Click Connect and the site enumerates.
9. Click Close and a list of published applications displays. Add some applications from the list, and then cick OK and Finish.



10. Right click on the policy and select Activate. You can rename the policy if you want to.

Configure Session Recording Player

Before a Session Recording Player can play sessions, you must configure it to connect to the Session Recording Server that stores the recorded sessions. Each Session Recording Player can be configured with the ability to connect to multiple Session Recording Servers, but can connect to only one Session Recording Server at a time. If the Player is configured with

the ability to connect to multiple Session Recording Servers, users can change which Session Recording Server the Player connects to by selecting a check box.

1. Log on to the workstation where Session Recording Player is installed.
2. Start the Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options.
4. In the Connections tab, click Add.
5. In the Hostname field, type the name or Internet protocol (IP) address of the computer hosting the Session Recording Server and select the protocol. By default Session Recording is configured to use HTTPS/SSL to secure communications. If SSL is not configured, select HTTP.
6. If you want to configure the Session Recording Player with the ability to connect to more than one Session Recording Server, repeat Steps 4 and 5 for each Session Recording Server.
7. Ensure that the check box for the Session Recording Server you want to connect to is selected.

Grant access rights to users

Feb 25, 2015

Note: For security reasons, grant users only the rights they need to perform specific functions, such as viewing recorded sessions.

You grant rights to Session Recording users by assigning them to roles using the Session Recording Authorization Console on the Session Recording Server. Session Recording users have three roles:

- **Player.** Grants the right to view recorded XenApp sessions. There is no default membership in this role.
- **PolicyQuery.** Allows the servers hosting the Session Recording Agent to request recording policy evaluations. By default, authenticated users are members of this role.
- **PolicyAdministrator.** Grants the right to view, create, edit, delete, and enable recording policies. By default, administrators of the computer hosting the Session Recording Server are members of this role.

Session Recording supports users and groups defined in Active Directory.

To assign users to roles

1. Log on to computer hosting the Session Recording Server, as administrator or as a member of the Policy Administrator role.
2. Start the Session Recording Authorization Console.
3. Select the role to which you want to assign users.
4. Choose Action > Assign Windows Users and Groups.
5. Add the users and groups.

Any changes made to the console take effect during the update that occurs once every minute.

Create and activate recording policies

Apr 23, 2015

Use the Session Recording Policy Console to create and activate policies that determine which sessions are recorded.

You can activate system policies available when Session Recording is installed or create and activate your own custom policies. Session Recording system policies apply a single rule to all users, published applications, and servers. Custom policies specifying which users, published applications, and servers are recorded.

The active policy determines which sessions are recorded. Only one policy is active at a time.

Use system policies

Session Recording provides these system policies:

- **Do not record**. If you choose this policy, no sessions are recorded. This is the default policy; if you do not specify another policy, no sessions are recorded.
- **Record everyone with notification**. If you choose this policy, all sessions are recorded. A pop-up window appears notifying the user that recording is occurring.
- **Record everyone without notification**. If you choose this policy, all sessions are recorded. A pop-up window does not appear notifying the user that recording is occurring.

System policies cannot be modified or deleted.

To activate a policy

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, expand Recording Policies.
5. Select the policy you want to make the active policy.
6. From the menu bar, choose Action > Activate Policy.

Create custom recording policies

When you create your own policy, you make rules to specify which users and groups, published applications, and servers have their sessions recorded. A wizard within the Session Recording Policy Console helps you create rules. To obtain the list of published applications and servers, you must have the site administrator read permission. Configure that on this site's Delivery Controller.

For each rule you create, you specify a recording action and a rule criteria. The recording action applies to sessions that meet the rule criteria.

For each rule, choose one recording action:

- Do not record. (Choose Disable session recording within the rules wizard.) This recording action specifies that sessions that meet the rule criteria are not recorded.
- Record with notification. (Choose Enable session recording with notification within the rules wizard.) This recording action specifies that sessions that meet the rule criteria are recorded. A pop-up window appears notifying the user that

recording is occurring.
- Record without notification. (Choose Enable session recording without notification within the rules wizard.) This recording action specifies that sessions that meet the rule criteria are recorded. Users are unaware that they are being recorded.

For each rule, choose at least one of the following to create the rule criteria:

- Users or Groups. You create a list of users or groups to which the recording action of the rule applies.
- Published Applications. You create a list of published applications to which the recording action of the rule applies. Within the rules wizard, choose the XenApp site or sites on which the applications are available.
- Applications Servers. You create a list of Server OS machines to which the recording action of the rule applies. Within the rules wizard, choose the XenApp site or sites where the servers reside.

When you create more than one rule in a recording policy, some sessions may match the criteria for more than one rule. In these cases, the rule with the highest priority is applied to the session.

The recording action of a rule determines its priority:

- Rules with the Do not record action have the highest priority
- Rules with the Record with notification action have the next highest priority
- Rules with the Record without notification action have the lowest priority

Some sessions may not meet any rule criteria in a recording policy. For these sessions, the recording action of the policies fallback rule applies. The recording action of the fallback rule is always Do not record. The fallback rule cannot be modified or deleted.

Using Active Directory Groups

Session Recording allows you to use Active Directory groups when creating policies. Using Active Directory groups instead of individual users simplifies creation and management of rules and policies. For example, if users in your company's finance department are contained in an Active Directory group named Finance, you can create a rule that applies to all members of this group by selecting the Finance group within the rules wizard when creating the rule.

White Listing Users

You can create Session Recording policies that ensure that the sessions of some users in your organization are never recorded. This is called white listing these users. White listing is useful for users who handle privacy-related information or when your organization does not want to record the sessions of a certain class of employees.

For example, if all managers in your company are members of an Active Directory group named Executive, you can ensure that these users' sessions are never recorded by creating a rule that disables session recording for the Executive group. While the policy containing this rule is active, no sessions of members of the Executive group are recorded. The sessions of other members of your organization are sessions recorded based on other rules in the active policy.

Create a new policy

Note: When using the rules wizard, you may be prompted to "click on underlined value to edit" when no underlined value appears. Underlined values appear only when applicable. If no underline values appear, ignore the step.

1. Log on to the server where Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session

Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, select Recording Policies.
5. From the menu bar, choose Action > Add New Policy. A policy called New Policy appears in the left pane.
6. Select the new policy and choose Action > Rename from the menu bar.
7. Type a name for the policy you are about to create and press Enter or click anywhere outside the new name.
8. With the policy selected, choose Action > Add New Rule from the menu bar to launch the rules wizard.
9. Follow the instructions to create the rules for this policy.

Modify a policy

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, expand Recording Policies.
5. Select the policy you want to modify. The rules for the policy appear in the right pane.
6. Add a new rule, modify a rule, or delete a rule:
   - From the menu bar, choose Action > Add New Rule. If the policy is active, a pop-up window appears requesting confirmation of the action. Use the rules wizard to create a new rule.
   - Select the rule you want to modify, right-click, and choose Properties. Use the rules wizard to modify the rule.
   - Select the rule you want to delete, right-click, and choose Delete Rule.

Delete a policy

Note: You cannot delete a system policy or a policy that is active.

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, expand Recording Policies.
5. In the left pane, select the policy you want to delete. If the policy is active, you must activate another policy.
6. From the menu bar, choose Action > Delete Policy.
7. Select Yes to confirm the action.

Understanding rollover behavior

When you activate a policy, the previously active policy remains in effect until the user's session ends; however, in some cases, the new policy takes effect when the file rolls over. Files roll over when they have reached the maximum size limit. For information on maximum file sizes for recordings, see Specify file size for recordings.

The following table details what happens when you apply a new policy while a session is being recorded and a rollover occurs:

If the previous policy was:	And the new policy is:	After a rollover the policy will be:
Do not record	Any other policy	No change. The new policy takes effect only when the user logs on to a new session.

If the previous policy was:	And the new policy is:	After a rollover the policy will be:
Record without notification	Do not record	Recording stops.
	Record with notification	Recording continues and a notification message appears.
Record with notification	Do not record	Recording stops.
	Record without notification	Recording continues. No message appears the next time a user logs on.

Disable or enable recording

Mar 24, 2015

You install the Session Recording Agent on each Server OS machine for which you want to record sessions. Within each agent is a setting that enables recording for the server on which it is installed. After recording is enabled, Session Recording evaluates the active recording policy, which determines which sessions are recorded.

When you install the Session Recording Agent, recording is enabled. Citrix recommends that you disable Session Recording on servers that are not recorded because they experience a small impact on performance, even if no recording takes place.

To disable or enable recording on a server

1. Log on to the server where the Session Recording Agent is installed.
2. From the Start menu, choose Session Recording Agent Properties.
3. Under Session Recording, select or clear the Enable session recording for this Server OS VDA check box to specify whether or not sessions can be recorded for this server.
4. When prompted, restart the Session Recording Agent Service to accept the change.

Note: When you install Session Recording, the active policy is Do not record (no sessions are recorded on any server). To begin recording, use the Session Recording Policy Console to activate a different policy.

Configure the connection to the Session Recording Server

Feb 02, 2015

The connection between the Session Recording Agent and the Session Recording Server is typically configured when the Session Recording Agent is installed. To configure this connection after Session Recording Agent is installed, use Session Recording Agent Properties.

1. Log on to the server where Session Recording Agent is installed.
2. From the Start menu, choose Session Recording Agent Properties.
3. Click the Connections tab.
4. In the Session Recording Server field, type the server name or its Internet protocol (IP) address.
5. In the Session Recording Storage Manager message queue section, select the protocol that is used by the Session Recording Storage Manager to communicate and modify the default port number, if necessary.
6. In the Message life field, accept the default of 7200 seconds (two hours) or type a new value for the number of seconds each message is retained in the queue if there is a communication failure. After this period of time elapses, the message is deleted and the file is playable until the point where the data is lost.
7. In the Session Recording Broker section, select the communication protocol the Session Recording Broker uses to communicate and modify the default port number, if necessary.
8. When prompted, restart the Session Recording Agent Service to accept the changes.

Create notification messages

Feb 02, 2015

If the active recording policy specifies that users are notified when their sessions are recorded, a pop-up window appears displaying a notification message after users type their credentials. The following message is the default notification: “Your activity with one or more of the programs you recently started is being recorded. If you object to this condition, close the programs.” The user clicks OK to dismiss the window and continue the session.

The default notification message appears in the language of the operating system of the computers hosting the Session Recording Server.

You can create custom notifications in languages of your choice; however, you can have only one notification message for each language. Your users see the notification message in the language corresponding to their user preferred locale settings.

To create a new notification message

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Notifications tab.
4. Click Add.
5. Choose the language for the message and type the new message. You can create only one message for each language.

After accepting and activating, the new message appears in the Language-specific notification messages box.

Enable custom event recording

Feb 25, 2015

Session Recording allows you to use third-party applications to insert custom data, known as events, into recorded sessions. These events appear when the session is viewed using the Session Recording Player. They are part of the recorded session file and cannot be modified after the session is recorded.

For example, an event might contain the following text: “User opened a browser.” Each time a user opens a browser during a session that is being recorded, the text is inserted into the recording at that point. When the session is played using the Session Recording Player, the viewer can locate and count the times that the user opened a browser by noting the number of markers that appear in the Events and Bookmarks list in the Session Recording Player.

To insert custom events into recordings on a server:

- Use Session Recording Agent Properties to enable a setting on each server where you want to insert custom events. You must enable each server separately; you cannot globally enable all servers in a site.
- Write applications built on the Event API that runs within each user’s XenApp session (to inject the data into the recording).

The Session Recording installation includes an event recording COM application (API) that allows you to insert text from third-party applications into a recording. You can use the API from many programming languages including Visual Basic, C++, or C#. The Session Recording Event API .dll is installed as part of the Session Recording installation. You can find it at C:\Program Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll.

To enable custom event recording on a server

1. Log on to the server where the Session Recording Agent is installed.
2. From the Start menu, choose Session Recording Agent Properties.
3. In Session Recording Agent Properties, click the Recording tab.
4. Under Custom event recording, select the Allow third party applications to record custom data on this XenApp server check box.

Enable or disable live session playback

Feb 25, 2015

Using Session Recording Player, you can view a session after or while it is being recorded. Viewing a session that is currently recording is similar to seeing actions happening live; however, there is actually a one to two second delay as the data propagates from the XenApp server.

Some functionality is not available when viewing sessions that have not completed recording:

- A digital signature cannot be assigned until recording is complete. If digital signing is enabled, you can view live playback sessions, but they are not digitally signed and you cannot view certificates until the session is completed.
- Playback protection cannot be applied until recording is complete. If playback protection is enabled, you can view live playback sessions, but they are not encrypted until the session is completed.
- You cannot cache a file until recording is complete.

By default, live session playback is enabled.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Playback tab.
4. Select or clear the Allow live session playback check box.

Enable or disable playback protection

Feb 02, 2015

As a security precaution, Session Recording automatically encrypts recorded files before they are downloaded for viewing in the Session Recording Player. This playback protection prevents them from being copied and viewed by anyone other than the user who downloaded the file. The files cannot be played back on another workstation or by another user. Encrypted files are identified with an .icle extension; unencrypted files are identified with an .icl extension. The files remain encrypted while they reside in the cache on the workstation where the Session Recording Player is installed until they are opened by an authorized user.

Citrix recommends that you use HTTPS to protect the transfer of data.

By default, playback protection is enabled.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Playback tab.
4. Select or clear the Encrypt session recording files downloaded for playback check box.

Enable and disable digital signing

Feb 02, 2015

If you installed certificates on the computers on which the Session Recording components are installed, you can enhance the security of your Session Recording deployment by assigning digital signatures to session recording.

By default, digital signing is disabled.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Signing tab.
4. Browse to the certificate that enables secure communication among the computers on which the Session Recording components are installed.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Signing tab.
4. Click Clear.

Specify where recordings are stored

Feb 03, 2015

Use Session Recording Server Properties to specify where recordings are stored and where archived recordings are restored.

Note: To archive files or restore deleted files, use the icldb command.

By default, recordings are stored in the drive:\SessionRecordings directory of the computer hosting the Session Recording Server. You can change the directory where the recordings are stored, add additional directories to load-balance across multiple volumes, or make use of additional space. Multiple directories in the list indicates recordings are load-balanced across the directories. You can add a directory multiple times. Load balancing cycles through the directories.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Storage tab.
4. Use the File storage directories list to manage the directories where recordings are stored.

You can create file storage directories on the local drive, the SAN volume, or a location specified by a UNC network path. Network mapped drive letters are not supported. Do not use Session Recording with Network-Attached Storage (NAS), due to serious performance and security problems associated with writing recording data to a network drive.

By default, archived recordings are restored to the drive:\SessionRecordingsRestore directory of the computer hosting the Session Recording Server. You can change the directory where the archived recordings are restored.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Storage tab.
4. In the Restore directory for archived files field, type the directory for the restored archive files.

Specify file size for recordings

Feb 02, 2015

As recordings grow in size, the files can take longer to download and react more slowly when you use the seek slider to navigate during playback. To control file size, specify a threshold limit for a file. When the recording reaches this limit, Session Recording closes the file and opens a new one to continue recording. This action is called a rollover.

You can specify two thresholds for a rollover:

- **File size.** When the file reaches the specified number of megabytes, Session Recording closes the file and opens a new one. By default, files roll over after reaching 50 megabytes; however, you can specify a limit from 10 megabytes to one gigabyte.
- **Duration.** After the session records for the specified number of hours, the file is closed and a new file is opened. By default, files roll over after recording for 12 hours; however, you can specify a limit from one to 24 hours.

Session Recording checks both fields to determine which event occurs first to determine when to rollover. For example, if you specify 17MB for the file size and six hours for the duration and the recording reaches 17MB in three hours, Session Recording reacts to the 17MB file size to close the file and open a new one.

To prevent the creation of many small files, Session Recording does not rollover until at least one hour elapses (this is the minimum number that you can enter) regardless of the value specified for the file size. The exception to this rule is if the file size surpasses one gigabyte.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Rollover tab.
4. Enter an integer between 10 and 1024 to specify the maximum file size in megabytes.
5. Enter an integer between 1 and 24 to specify the maximum recording duration in hours.

View recordings

Feb 25, 2015

Use Session Recording Player to view, search, and bookmark recorded XenApp or XenDesktop sessions.

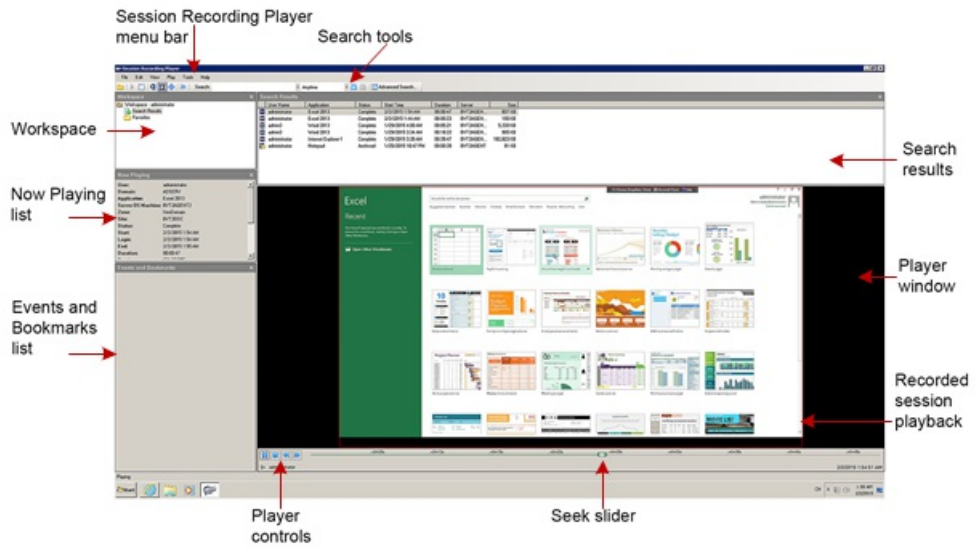
If sessions are recorded with the live playback feature enabled, you can view sessions that are in progress, with a delay of a few seconds, as well as sessions that are completed.

Sessions that have a longer duration or larger file size than the limits configured by your Session Recording administrator appear in more than one session file.

Note: A Session Recording administrator must grant users the right to access to recorded Server OS machine sessions. If you are denied access to viewing sessions, contact your Session Recording administrator.
When Session Recording Player is installed, the Session Recording administrator typically sets up a connection between the Session Recording Player and a Session Recording Server. If this connection is not set up, the first time you perform a search for files, you are prompted to set it up. Contact your Session Recording administrator for set up information.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
   The Session Recording Player appears.

This illustration shows the Session Recording Player with callouts indicating its major elements. The functions of these elements are described throughout following articles.



The Session Recording Player has window elements that toggle on and off.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose View.
4. Choose the elements that you want to display. Selecting an element causes it to appear immediately. A check mark indicates that the element is selected.

If the Session Recording administrator set up your Session Recording Player with the ability to connect to more than one Session Recording Server, you can select the Session Recording Server that the Session Recording Player connects to. The Session Recording Player can connect to only one Session Recording Server at a time.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Connections.
4. Select the Session Recording Server to which you want to connect.

Open and play recordings

Feb 04, 2015

You can open session recordings in Session Recording Player in three ways:

- Perform a search using the Session Recording Player. Recorded sessions that meet the search criteria appear in the search results area.
- Access recorded session files directly from your local disk drive or a share drive.
- Access recorded session files from a Favorites folder

When you open a file that was recorded without a digital signature, a warning appears telling you that the origin and integrity of the file was not verified. If you are confident of the integrity of the file, click Yes in the warning pop-up window to open the file.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Perform a search.
4. If the search results area is not visible, select Search Results in the Workspace pane.
5. In the search results area, select the session you want to play.
6. Do any of the following:
   - Double-click the session
   - Right-click and select Play
   - From the Session Recording Player menu bar, select Play > Play

Recorded session file names begin with an i_, followed by a unique alphanumeric file ID, followed by the .icl and .icle file extension: .icl for recordings without playback protection applied, .icle for recordings with playback protection applied. Session Recording saves recorded session files in a directory structure that incorporates the date the session was recorded. For example, the file for a session recorded on December 22, 2014, is saved in folder path 2014\12\22.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Do any of the following:
   - From the Session Recording Player menu bar, select File > Open and browse for the file
   - Using Windows Explorer, navigate to the file and drag the file into the Player window
   - Using Windows Explorer, navigate to and double-click the file
   - If you created Favorites in the Workspace pane, select Favorites and open the file from the Favorites area in the same way you open files from the search results area

Creating Favorites folders allows you to quickly access recordings that you view frequently. These Favorites folders reference recorded session files that are stored on your workstation or on a network drive. You can import and export these files to other workstations and share these folders with other Session Recording Player users.

Note: Only users with access rights to Session Recording Player can download the recorded session files associated with Favorites folders. Contact your Session Recording administrator for access rights.

To create a Favorites subfolder:

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. In the Session Recording Player, select the Favorites folder in your Workspace pane.
4. From the menu bar, choose File > Folder > New Folder. A new folder appears under the Favorites folder.
5. Type the folder name, then press Enter or click anywhere to accept the new name.

Use the other options that appear in the File > Folder menu to delete, rename, move, copy, import, and export the folders.

Search for recorded sessions

Mar 24, 2015

Session Recording Player allows you to perform quick searches, perform advanced searches, and specify options that apply to all searches. Results of searches appear in the search results area of the Session Recording Player.

Note: To display all available recorded sessions, up to the maximum number of sessions that may appear in a search, perform a search without specifying any search parameters.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Define your search criteria:
   - Enter a search criterion in the Search field. To assist you:
   - Move the mouse pointer over the Search label to display a list of parameters to use as a guideline
   - Click the arrow to the right of the Search field to display the text for the last 64 searches you performed
   - Use the drop-down list to the right of the Search field to select a period or duration specifying when the session was recorded.
4. Click the binocular icon to the right of the drop-down list to start the search.

Tip: Advanced searches might take up to 20 seconds to return results containing more than 150K entities. Citrix recommends using more accurate search conditions such as a date range or user to reduce the result number.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. In the Session Recording Player window, click Advanced Search on the tool bar or choose Tools > Advanced Search.
4. Define your search criteria in the tabs of the Advanced Search dialog box:
   - Common allows you to search by domain or account authority, site, group, Server OS machine, application, or file ID.
   - Date/Time allows you to search date, day of week, and time of day.
   - Events allows you to search on custom events that your Session Recording administrator inserted to the sessions.
   - Other allows you to search by session name, client name, client address, and recording duration. It also allows you to specify, for this search, the maximum number of search results displayed and whether or not archived files are included in the search.

   As you specify search criteria, the query you are creating appears in the pane at the bottom of the dialog box.
5. Click Search to start the search.

Tip: You can save and retrieve advanced search queries. Click Save within the Advanced Search dialog box to save the current query. Click Open within the Advanced Search dialog box to retrieve a saved query. Queries are saved as files with an .isq extension.

Session Recording Player search options allow you to limit maximum number of session recordings that appear in search results and to specify whether or not search results include archived session files.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Search.
4. In the Maximum result to display field, type the number of search results you want to display. A maximum of 500 results

can be displayed.

5. To set whether or not archived files are included in searches, select or clear Include archived files.

Play recorded sessions

Mar 23, 2015

After you open a recorded session in the Session Recording Player, you can navigate through the recorded sessions using these methods:

- Use the player controls to play, stop, pause, and increase or decrease playback speed
- Use the seek slider to move forward or backward

If you have inserted markers into the recording or if the recorded session contains custom events, you can also navigate through the recorded session by going to those markers and events.

Note:

- During playback of a recorded session, a second mouse pointer may appear. The second pointer appears at the point in the recording when the user navigated within Internet Explorer and clicked an image that was originally larger than the screen but was scaled down automatically by Internet Explorer. While only one pointer appears during the session, two may appear during playback.
- This version of Session Recording does not support SpeedScreen Multimedia Acceleration for XenApp or the Flash quality adjustment policy setting for XenApp. When this option is enabled, playback displays a black square.
- Session Recording cannot record the Lync webcam video when using the HDX RealTime Optimization Pack for Microsoft Lync.

You can click the player controls under the Player window or access them by choosing Play from the Session Recording Player menu bar. Use Player controls to:

	Play the selected session file.
	Pause playback.
	Stop playback. If you click Stop, then Play, the recording restarts at the beginning of the file.
	Halve the current playback speed down to a minimum of one-quarter normal speed.
	Double the current playback speed up to a maximum of 32 times normal speed.

Use the seek slider below the Player window to jump to a different position within the recorded session. You can drag the seek slider to the point in the recording you want to view or click anywhere on the slider bar to move to that location.

You can also use the following keyboard keys to control the seek slider:

Key:	Seek action:

Key:	Seek action:
Home	Seek to the beginning.
End	Seek to the end.
Right Arrow	Seek forward five seconds.
Left Arrow	Seek backward five seconds.
Move mouse wheel one notch down	Seek forward 15 seconds.
Move mouse wheel one notch up	Seek backward 15 seconds.
Ctrl + Right Arrow	Seek forward 30 seconds.
Ctrl + Left Arrow	Seek backward 30 seconds.
Page Down	Seek forward one minute.
Page Up	Seek backward one minute.
Ctrl + Move mouse wheel one notch down	Seek forward 90 seconds.
Ctrl + Move mouse wheel one notch up	Seek backward 90 seconds.
Ctrl + Page Down	Seek forward six minutes.
Ctrl + Page Up	Seek backward six minutes.

Note: To adjust the speed of the seek slider: From the Session Recording Player menu bar, choose Tools > Options > Player and drag the slider to increase or decrease the seek response time. A faster response time requires more memory. The response might be slow depending on the size of of the recordings and your machine's hardware.

You can set Session Recording Player to play recorded sessions in exponential increments from one-quarter normal playback speed to 32 times normal playback speed.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Play > Play Speed.
4. Choose a speed option.

The speed adjusts immediately. A number indicating the increased or decreased speed appears below the Player window

controls. Text indicating the exponential rate appears briefly in green in the Player window.

Fast review mode allows you to set Session Recording Player to skip the portions of recorded sessions in which no action takes place. This setting saves time for playback viewing; however, it does not skip animated sequences such as animated mouse pointers, flashing cursors, or displayed clocks with second hand movements.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Play > Fast Review Mode.

The option toggles on and off. Each time you choose it, its status appears briefly in green in the Player window.

Use events and bookmarks

Feb 02, 2015

You can use events and bookmarks to help you navigate through recorded sessions.

Events are inserted to sessions as they are recorded, using the Event API and a third-party application. Events are saved as part of the session file. You cannot delete or alter them using the Session Recording Player.

Bookmarks are markers you insert into the recorded sessions using the Session Recording Player. Bookmarks are associated with the recorded session until you delete them, but they are not saved as part of the session file. By default, each bookmark is labeled with the text Bookmark, but you can change this to any text annotation up to 128 characters long.

Events and bookmarks appear as dots under the Player window. Events appear as yellow dots; bookmarks appear as blue dots. Moving the mouse over these dots displays the text label associated with them. You can also display the events and bookmarks in the events and bookmarks list of the Session Recording Player. They appear in this list with their text labels and the times in the recorded session at which they appear, in chronological order.

You can use events and bookmarks to help you navigate through recorded sessions. By going to an event or bookmark, you can skip to the point in the recorded session where the event or bookmark is inserted.

The events and bookmarks list displays the events and bookmarks inserted in the recorded session that is currently playing. It can show events only, bookmarks only, or both.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Move the mouse pointer into the events and bookmarks list area and right-click to display the menu.
4. Choose Show Events Only, Show Bookmarks Only, or Show All.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Begin playing the recorded session to which you want to add a bookmark.
4. Move the seek slider to the position where you want to insert the bookmark.
5. Move the mouse pointer into the Player window area and right-click to display the menu.
6. Add a bookmark with the default label Bookmark or create an annotation:
   - To add a bookmark with the default label Bookmark, choose Add Bookmark.
   - To add a bookmark with a descriptive text label that you create, choose Add Annotation. Type the text label you want to assign to the bookmark, up to 128 characters. Click OK.

After a bookmark is created, you can add an annotation to it or change its annotation.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Begin playing the recorded session containing the bookmark.
4. Ensure that the events and bookmarks list is displaying bookmarks.
5. Select the bookmark in the events and bookmarks list and right-click to display the menu.

6. Choose Edit Annotation.
7. In the window that appears, type the new annotation and click OK.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Begin playing the recorded session containing the bookmark.
4. Ensure that the events and bookmarks list is displaying bookmarks.
5. Select the bookmark in the events and bookmarks list and right-click to display the menu.
6. Choose Delete.

Going to an event or bookmark causes the Session Recording Player to go to the point in the recorded session where the event or bookmark is inserted.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Begin playing a session recording containing events or bookmarks.
4. Go to an event or bookmark:
   - In the area below the Player window, click the dot representing the event or bookmark to go to the event or bookmark.
   - In the events and bookmarks list, double-click the event or bookmark to go to it. To go to the next event or bookmark, select any event or bookmark from the list, right-click to display the menu, and choose Seek to Bookmark.

Change the playback display

Feb 02, 2015

Options allow you to change how recorded sessions appear in the Player window. You can pan and scale the image, show the playback in full-screen mode, display the Player window in a separate window, and display a red border around the recorded session to differentiate it from the Player window background.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose View > Player Full Screen.
4. To return to the original size, press ESC or F11.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose View > Player in Separate Window. A new window appears containing the Player window. You can drag and resize the window.
4. To embed the Player window in the main window, choose View > Player in Separate Window, or press F10.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Play > Panning and Scaling > Scale to Fit.
   - Scale to Fit (Fast Rendering) shrinks the image while providing a good quality image. Images are drawn quicker than when using the High Quality option but the images and text are not as sharp. Use this option if you are experiencing performance issues when using the High Quality mode.
   - Scale to Fit (High Quality) shrinks the image while providing high quality images and text. Using this option may cause the images to be drawn more slowly than the Fast Rendering option.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Play > Panning and Scaling > Panning. The pointer changes to a hand and a small representation of the screen appears in the top right of the Player window.
4. Drag the image. The small representation indicates where you are in the image.
5. To stop panning, choose one of the scaling options.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Player from the menu bar.
4. Select the Show border around session recording check box.
   Tip: If the Show border around session recording check box is not selected, you can temporarily view the red border by

clicking and holding down the left mouse button while the pointer is in the Player window.

Cache recorded session files

Feb 02, 2015

Each time you open a recorded session file, the Session Recording Player downloads the file from the location where the recordings are stored. If you download the same files frequently, you can save download time by caching the files on your workstation. Cached files are stored on your workstation in this folder:

userprofile\AppData\Local\Citrix\SessionRecording\Player\Cache

You can specify how much disk space is used for the cache. When the recordings fill the specified disk space, Session Recording deletes the oldest, least used recordings to make room for new recordings. You can empty the cache at any time to free up disk space.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Cache.
4. Select the Cache downloaded files on local machine check box.
5. If you want to limit the amount of disk space used for caching, select the Limit amount of disk space to use check box and specify the number of megabytes to be used for cache.
6. Click OK.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Cache.
4. Select the Cache downloaded files on local machine check box.
5. In the Session Recording Player, choose Tools > Options > Cache.
6. Click Purge Cache, then OK to confirm the action.

Troubleshooting Session Recording

Mar 24, 2015

This troubleshooting information contains solutions to some issues you may encounter during and after installing Session Recording components:

- Components failing to connect to each other
- Sessions failing to record
- Problems with the Session Recording Player or Session Recording Policy Console
- Issues involving your communication protocol

When Session Recording Agent cannot connect, the Exception caught while sending poll messages to Session Recording Broker event message is logged, followed by the exception text. The exception text provides the reason why the connection failed. These reasons include:

- The underlying connection was closed. Could not establish a trust relationship for the SSL/TLS secure channel. This exception means that the Session Recording Server is using a certificate that is signed by a CA that the server on which the Session Recording Agent resides does not trust, or have a CA certificate for. Alternatively, the certificate may have expired or been revoked.

  Resolution: Verify that the correct CA certificate is installed on the server hosting the Session Recording Agent or use a CA that is trusted.

- The remote server returned an error: (403) forbidden. This is a standard HTTPS error displayed when you attempt to connect using HTTP (nonsecure protocol). The computer hosting the Session Recording Server rejects the connection because it accepts only secure connections.

  Resolution: Use Session Recording Agent Properties to change the Session Recording Broker protocol to HTTPS.

The Session Recording Broker returned an unknown error while evaluating a record policy query. Error code 5 (Access Denied). See the Event log on the Session Recording Server for more details. This error occurs when sessions are started and a request for a record policy evaluation is made. The error is a result of the Authenticated Users group (this is the default member) being removed from the Policy Query role of the Session Recording Authorization Console.

Resolution: Add the Authenticated Users group back into this role, or add each server hosting each Session Recording Agent to the PolicyQuery role.

The underlying connection was closed. A connection that was expected to be kept alive was closed by the server. This error means that the Session Recording Server is down or unavailable to accept requests. This could be due to IIS being offline or restarted, or the entire server may be offline.

Resolution: Verify that the Session Recording Server is started, IIS is running on the server, and the server is connected to the network.

When the Session Recording Server cannot connect to the Session Recording Database, you may see a message similar to one of the following:

Event Source:

Citrix Session Recording Storage Manager Description: Exception caught while establishing database connection. This error appears in the applications event log in the Event Viewer of the computer hosting the Session Recording Server.

Unable to connect to the Session Recording Server. Ensure that the Session Recording Server is running. This error message appears when you launch the Session Recording Policy Console.

Resolution:

- The Express Edition of Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, or Microsoft SQL Server 2014 is installed on a stand-alone server and does not have the correct services or settings configured for Session Recording. The server must have TCP/IP protocol enabled and SQL Server Browser service running. See the Microsoft documentation for information about enabling these settings.
- During the Session Recording installation (administration portion), incorrect server and database information was given. Uninstall the Session Recording Database and reinstall it, supplying the correct information.
- The Session Recording Database Server is down. Verify that the server has connectivity.
- The computer hosting the Session Recording Server or the computer hosting the Session Recording Database Server cannot resolve the FQDN or NetBIOS name of the other. Use the ping command to verify the names can be resolved.

Logon failed for user 'NT_AUTHORITY\ANONYMOUS LOGON'. This error message means that the services are logged on incorrectly as .\administrator.

Resolution: Restart the services as local system user and restart the SQL services.

If your application sessions are not recording successfully, start by checking the application event log in the Event Viewer on the Server OS machine running the Session Recording Agent and Session Recording Server. This may provide valuable diagnostic information.

If sessions are not recording, these issues might be the cause:

- **Component connectivity and certificates**. If the Session Recording components cannot communicate with each other, this can cause session recordings to fail. To troubleshoot recording issues, verify that all components are configured correctly to point to the correct computers and that all certificates are valid and correctly installed.
- **Non-Active Directory domain environments**. Session Recording is designed to run in a Microsoft Active Directory domain environment. If you are not running in an Active Directory environment, you may experience recording issues. Ensure that all Session Recording components are running on computers that are members of an Active Directory domain.
- **Session sharing conflicts with the active policy.** Session Recording matches the active policy with the first published application that a user opens. Subsequent applications opened during the same session continue to follow the policy that is in force for the first application. To prevent session sharing from conflicting with the active policy, publish the conflicting applications on separate Server OS machines.
- **Recording is not enabled.** By default, installing the Session Recording Agent on a Server OS machine enables the server for recording. Recording will not occur until an active recording policy is configured to allow this.
- **The active recording policy does not permit recording.** For a session to be recorded, the active recording policy must permit the sessions for the user, server, or published application to be recorded.
- **Session Recording services are not running.** For sessions to be recorded, the Session Recording Agent service must be running on the Server OS machine and the Session Recording Storage Manager service must be running on the computer hosting the Session Recording Server.

- **MSMQ is not configured.** If MSMQ is not correctly configured on the server running the Session Recording Agent and the computer hosting the Session Recording Server, recording problems may occur.

If you experience difficulties when viewing recordings using the Session Recording Player, the following error message may appear on the screen:

Download of recorded session file failed. Live session playback is not permitted. The server has been configured to disallow this feature. This error indicates that the server is configured to disallow the action.

Resolution: In the Session Recording Server Properties dialog box, choose the Playback tab and select the Allow live session playback check box.

When recordings are becoming corrupt or incomplete when viewing them using the Session Recording Player, you may also see warnings in the Event logs on the Session Recording Agent.

Event Source: Citrix Session Recording Storage Manager

Description: Data lost while recording file <icl file name>

This usually happens when Machine Creation Services (MCS) or Provisioning Services is used to create VDAs with a configured master image and Microsoft Message Queuing (MSMQ) installed. In this condition the VDAs have the same QMIds for MSMQ.

Resolution: Create the unique QMId for each VDA. A workaround is introduced in Known Issues.

When you install Session Recording Database or Session Recording Server, the test connection fails with the error message **Database connection test failed. Please correct Database instance name** even if the database instance name is correct.

Resolution: Make sure the current user has the public SQL Server role permission to correct the permission limitation failure.

Verify component connections

Apr 22, 2015

During the setup of Session Recording, the components may not connect to other components. All the components communicate with the Session Recording Server (Broker). By default, the Broker (an IIS component) is secured using the IIS default Web site certificate. If one component cannot connect to the Session Recording Server, the other components may also fail when attempting to connect.

The Session Recording Agent and Session Recording Server (Storage Manager and Broker) log connection errors in the applications event log in the Event Viewer of the computer hosting the Session Recording Server, while the Session Recording Policy Console and Session Recording Player display connection error messages on screen when they fail to connect.

1. Log on to the server where the Session Recording Agent is installed.
2. From the Start menu, choose Session Recording Agent Properties.
3. In Session Recording Server Properties, click Connection.
4. Verify that the value for Session Recording Server is the correct server name of the computer hosting the Session Recording Server.
5. Verify that the server given as the value for Session Recording Server can be contacted by the Server OS machine.

Note: Check the application event log for errors and warnings.

Caution: Using Registry Editor can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

1. Log on to the computer hosting the Session Recording Server.
2. Open the Registry Editor.
3. Browse to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Verify the value of SmAudDatabaseInstance correctly references the Session Recording Database you installed in your SQL Server instance.

1. Using a SQL Management tool, open your SQL instance that contains the Session Recording Database you installed.
2. Open the Security permissions of the Session Recording Database.
3. Verify the Session Recording Computer Account has access to the database. For example, if the computer hosting the Session Recording Server is named SsRecSrv in the MIS domain, the computer account in your database should be configured as MIS\SsRecSrv$. This value is configured during the Session Recording Database install.

Testing connections to the Session Recording Server IIS site by using a Web browser to access the Session Recording Broker Web page can help you determine whether problems with communication between Session Recording components stem from misconfigured protocol configuration, certification issues, or problems starting Session Recording Broker.

To verify IIS connectivity for the Session Recording Agent

1. Log on to the server where the Session Recording Agent is installed.
2. Launch a Web browser and type the following address:
   - For HTTPS: https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl, where servername is the name of the computer hosting the Session Recording Server
   - For HTTP: http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl, where servername is the name of the computer hosting the Session Recording Server
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

If you see an XML document within your browser, this verifies that the computer running the Session Recording Agent is connected to the computer hosting the Session Recording Server using the configure protocol.

To verify IIS connectivity for the Session Recording Player

1. Log on to the workstation where the Session Recording Player is installed.
2. Launch a Web browser and type the following address:
   - For HTTPS: https://servername/SessionRecordingBroker/Player.rem?wsdl, where servername is the name of the computer hosting the Session Recording Server
   - For HTTP: http://servername/SessionRecordingBroker/Player.rem?wsdl, where servername is the name of the computer hosting the Session Recording Server
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

If you see an XML document within your browser, this verifies that the computer running the Session Recording Player is connected to the computer hosting the Session Recording Server using the configure protocol.

To verify IIS connectivity for the Session Recording Policy Console

1. Log on to the server where the Session Recording Policy Console is installed.
2. Launch a Web browser and type the following address:
   - For HTTPS: https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl, where servername is the name of the computer hosting the Session Recording Server
   - For HTTP: http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl, where servername is the name of the computer hosting the Session Recording Server
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

If you see an XML document within your browser, this verifies that the computer running the Session Recording Policy Console is connected to the computer hosting the Session Recording Server using the configure protocol.

If you are using HTTPS as your communication protocol, the computer hosting the Session Recording Server must be configured with a server certificate. All component connections to the Session Recording Server must have root certificate authority (CA). Otherwise, attempted connections between the components fail.

You can test your certificates by accessing the Session Recording Broker Web page as you would when testing IIS connectivity. If you are able to access the XML page for each component, the certificates are configured correctly.

Here are some common ways certificate issues cause connections to fail:

- **Invalid or missing certificates.** If the server running the Session Recording Agent does not have a root certificate to trust the server certificate, cannot trust and connect to the Session Recording Server over HTTPS, causing connectivity to fail. Verify that all components trust the server certificate on the Session Recording Server.
- **Inconsistent naming.** If the server certificate assigned to the computer hosting the Session Recording Server is

created using a fully qualified domain name (FQDN), then all connecting components must use the FQDN when connecting to the Session Recording Server. If a NetBIOS name is used, configure the components with a NetBIOS name for the Session Recording Server.

- **Expired certificates.** If a server certificate expired, connectivity to the Session Recording Server through HTTPS fails. Verify the server certificate assigned to the computer hosting the Session Recording Server is valid and has not expired. If the same certificate is used for the digital signing of session recordings, the event log of the computer hosting the Session Recording Server provides error messages that the certificate expired or warning messages when it is about to expire.

Search for recordings if the Session Recording Player fails

Feb 04, 2015

If you experience difficulties when searching for recordings using the Session Recording Player, the following error messages may appear on the screen:

- Search for recorded session files failed. The remote server name could not be resolved: servername. where servername is the name of the server to which the Session Recording Player is attempting to connect. The Session Recording Player cannot contact the Session Recording Server. Two possible reasons for this are an incorrectly typed server name or the DNS cannot resolve the server name.
  Resolution: From the Player menu bar, choose Tools > Options > Connections and verify that the server name in the Session Recording Servers list is correct. If it is correct, from a command prompt, run the ping command to see if the name can be resolved. When the Session Recording Server is down or offline, the search for recorded session files failed error message is Unable to contact the remote server.
- Unable to contact the remote server. This error occurs when the Session Recording Server is down or offline.
  Resolution: Verify that the Session Recording Server is connected.
- Access denied error. An access denied error can occur if the user was not given permission to search for and download recorded session files.
  Resolution: Assign the user to the Player role using the Session Recording Authorization Console.
- Search for recorded session files failed. The underlying connection was closed. Could not establish a trust relationship for the SSL/TLS secure channel. This exception is caused by the Session Recording Server using a certificate that is signed by a CA that the client device does not trust or have a CA certificate for.
  Resolution: Install the correct or trusted CA certificate workstation where the Session Recording Player is installed.
- The remote server returned an error: (403) forbidden. This error is a standard HTTPS error that occurs when you attempt to connect using HTTP (nonsecure protocol). The server rejects the connection because, by default, it is configured to accept only secure connections.
  Resolution: From the Session Recording Player menu bar, choose Tools > Options > Connections. Select the server from the Session Recordings Servers list, then click Modify. Change the protocol from HTTP to HTTPS.

If your users see the notification message but the viewer cannot find the recordings after performing a search in the Session Recording Player, there could be a problem with MSMQ. Verify that the queue is connected to the Session Recording Server (Storage Manager) and use a Web browser to test for connection errors (if you are using HTTP or HTTPS as your MSMQ communication protocol).

To verify that the queue is connected:

1. Log on to the server hosting the Session Recording Agent and view the outgoing queues.
2. Verify that the queue to the computer hosting the Session Recording Server has a connected state.
   - If the state is “waiting to connect,” there are a number of messages in the queue, and the protocol is HTTP or HTTPS (corresponding to the protocol selected in the Connections tab in the Session Recording Agent Properties dialog box), perform Step 3.

- If state is “connected” and there are no messages in the queue, there may be a problem with the server hosting the Session Recording Server. Skip Step 3 and perform Step 4.

3. If there are a number of messages in the queue, launch a Web browser and type the following address:
   - For HTTPS: https://servername/msmq/private$/CitrixSmAudData, where servername is the name of the computer hosting the Session Recording Server
   - For HTTP: http://servername/msmq/private$/CitrixSmAudData, where servername is the name of the computer hosting the Session Recording Server

   If the page returns an error such as The server only accepts secure connections, change the MSMQ protocol listed in the Session Recording Agent Properties dialog box to HTTPS. Otherwise, if the page reports a problem with the Web site’s security certificate, there may be a problem with a trust relationship for the SSL/TLS secure channel. In that case, install the correct CA certificate or use a CA that is trusted.

4. If there are no messages in the queue, log on to the computer hosting the Session Recording Server and view private queues. Select citrixsmauddata. If there are a number of messages in the queue (Number of Messages Column), verify that the Session Recording StorageManager service is started. If it is not, restart the service.

Change your communication protocol

Feb 03, 2015

For security reasons, Citrix does not recommend using HTTP as a communication protocol. The Session Recording installation is configured to use HTTPS. If you want to use HTTP instead of HTTPS, you must change several settings.

1. Log on to the computer hosting the Session Recording Server and disable secure connections for Session Recording Broker in IIS.
2. Change the protocol setting from HTTPS to HTTP in each Session Recording Agent Properties dialog box:
    1. Log on to each server where the Session Recording Agent is installed.
    2. From the Start menu, choose Session Recording Agent Properties.
    3. In Session Recording Agent Properties, choose the Connections tab.
    4. In the Session Recording Broker area, select HTTP from the Protocol drop-down list and choose OK to accept the change. If you are prompted to restart the service, choose Yes.
3. Change the protocol setting from HTTPS to HTTP in the Session Recording Player settings:
    1. Log on to each workstation where the Session Recording Player is installed.
    2. From the Start menu, choose Session Recording Player.
    3. From the Session Recording Player menu bar, choose Tools > Options > Connections, select the server and choose Modify.
    4. Select HTTP from the Protocol drop-down list and click OK twice to accept the change and exit the dialog box.
4. Change the protocol setting from HTTPS to HTTP in the Session Recording Policy Console:
    1. Log on to the server where the Session Recording Policy Console is installed.
    2. From the Start menu, choose Session Recording Policy Console.
    3. Choose HTTP from the Protocol drop-down list and choose OK to connect. If the connection is successful, this setting is remembered the next time you launch the Session Recording Policy Console.

1. Log on to the computer hosting the Session Recording Server and enable secure connections for the Session Recording Broker in IIS.
2. Change the protocol setting from HTTP to HTTPS in each Session Recording Agent Properties dialog box:
    1. Log on to each server where the Session Recording Agent is installed.
    2. From the Start menu, choose Session Recording Agent Properties.
    3. In Session Recording Agent Properties, choose the Connections tab.
    4. In the Session Recording Broker area, select HTTPS from the Protocol drop-down list and choose OK to accept the change. If you are prompted to restart the service, choose Yes.
3. Change the protocol setting from HTTP to HTTPS in the Session Recording Player settings:
    1. Log on to each workstation where the Session Recording Player is installed.
    2. From the Start menu, choose Session Recording Player.
    3. From the Session Recording Player menu bar, choose Tools > Options > Connections, select the server and choose Modify.
    4. Select HTTPS from the Protocol drop-down list and click OK twice to accept the change and exit the dialog box.
4. Change the protocol setting from HTTP to HTTPS in the Session Recording Policy Console:
    1. Log on to the server where the Session Recording Policy Console is installed.
    2. From the Start menu, choose Session Recording Policy Console.

3. Choose HTTPS from the Protocol drop-down list and choose OK to connect. If the connection is successful, this setting is remembered the next time you launch the Session Recording Policy Console.

Reference: Manage your database records

Feb 03, 2015

The ICA Log database (ICLDB) utility is a database command-line utility used to manipulate the session recording database records. This utility is installed during the Session Recording installation in the drive:\Program Files\Citrix\SessionRecording\Server\Bin directory at the server hosting the Session Recording Server software.

The following table lists the commands and options that are available for the ICLDB utility. Type the commands using the following format:

icldb [version | locate | dormant | import | archive | remove | removeall] command-options [/l] [/f] [/s] [/?]

Note: More extensive instructions are available in the help associated with the utility. To access the help, from a command prompt, type drive:\Program Files\Citrix\SessionRecording\Server\Bin directory, type icldb /?. To access help for specific commands, type icldb command /?.

Command	Description
archive	Archives the session recording files older than the retention period specified. Use this command to archive files.
dormant	Displays or counts the session recording files that are considered dormant. Dormant files are session recordings that were not completed due to data loss. Use this command to verify if you suspect that you are losing data. You can verify if the session recording files are becoming dormant for the entire database, or only recordings made within the specified number of days, hours, or minutes.
import	Imports session recording files into the Session Recording database. Use this command to rebuild the database if you lose database records. Additionally, use this command to merge databases (if you have two databases, you can import the files from one of the databases).
locate	Locates and displays the full path to a session recording file using the file ID as the criteria. Use this command when you are looking for the storage location of a session recording file. It is also one way to verify if the database is up-to-date with a specific file.
remove	Removes the references to session recording files from the database. Use this command (with caution) to clean up the database. Specify the retention period to be used as the criteria. You can also remove the associated physical file.

Command	Description
removeall	Removes all of the references to session recording files from the Session Recording Database and returns the database to its original state. The actual physical files are not deleted; however you cannot search for these files in the Session Recording Player. Use this command (with caution) to clean up the database. Deleted references can be reversed only by restoring from your backup.
version	Displays the Session Recording Database schema version.
/l	Logs the results and errors to the Windows event log.
/f	Forces the command to run without prompts.
/s	Suppresses the copyright message.
/?	Displays help for the commands.

Third Party Notices

Jun 15, 2015

Session Recording may include third party software components licensed under the following terms. This list was generated using third party software as of the date listed. This list may change with specific versions of the product and may not be complete; it is provided “As-Is.” TO THE EXTENT PERMITTED BY APPLICABLE LAW, CITRIX AND ITS SUPPLIERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, WITH REGARD TO THE LIST OR ITS ACCURACY OR COMPLETENESS, OR WITH RESPECT TO ANY RESULTS TO BE OBTAINED FROM USE OR DISTRIBUTION OF THE LIST. BY USING OR DISTRIBUTING THE LIST, YOU AGREE THAT IN NO EVENT SHALL CITRIX BE HELD LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY OTHER DAMAGES WHATSOEVER RESULTING FROM ANY USE OR DISTRIBUTION OF THIS LIST.

MMC .NET Library

Licensed under the Common Public License, Version 1.0

Personal vDisk

Jul 07, 2014

You can use a diagnostic tool to monitor the changes made by users to both parts of their Personal vDisks (the user data and the application parts). These changes include applications that users have installed and files they have modified. The changes are stored in a set of reports.

1. On the machine that you want to monitor, run C:\Program Files\Citrix\personal vDisk\bin\CtxPvdDiag.exe.
2. Browse to a location where you want to store the reports and logs, select which reports to generate, and click OK. The following reports are available:

Report or Log	Generated Files	Changes Monitored
Software hive report	Software.Dat.Report.txt, Software.Dat.delta.txt	Software.Dat.Report.txt records the changes made by the user to the HKEY_LOCAL_MACHINE\Software hive. It consists of the following sections: • **List of Applications installed on the base** — The applications that were installed in Layer 0. • **List of user installed software** — the applications that were installed by the user on the application part of the vDisk. • **List of software uninstalled by user** — the applications removed by the user that were originally present in Layer 0. See Hive delta report for information on Software.Dat.delta.txt.
System hive report	SYSTEM.CurrentControlSet.DAT.Report.txt	This file records the changes made by the user to the HKEY_LOCAL_MACHINE\System hive. It contains the following sections: • **List of user installed services** — the services and drivers installed by the user. • **Startup of following services were changed** — the services and drivers whose start type was modified by the user.
Security hive report	SECURITY.DAT.Report.txt	This file monitors all changes that the user makes in the HKEY_LOCAL_MACHINE\Security hive.
Security Account Manager(SAM) hive report	SAM.DAT.Report.txt	This file monitors all changes that the user makes in the HKEY_LOCAL_MACHINE\SAM hive.
Hive delta	Software.Dat.delta.txt	This file records all registry keys and values added or

Report or Log	Generated Files	Changes Monitored
report		removed, and all values modified, by the user in the HKEY_LOCAL_MACHINE\Software hive.
Personal vDisk logs	Pud-IvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-IvmSupervisor.log, vDeskService-<#>.log	These files are generated by default in P:\Users\<user account>\AppData\Local\Temp\PVDLOGS but are moved to the selected location.
Windows operating system (OS) log	EvtLog_App.xml, EvtLog_System.xml, setupapi.app.log, setuperr.log, setupapi.dev.log, msinfo.txt	EvtLog_App.xml and EvtLog_System.xml are the application and system event logs in XML format from the Personal vDisk volume. Setupapi.app.log and setuperr.log contain log messages from when msiexec.exe was run during Personal vDisk installation. Setupapi.dev.log contains device installation log messages. Msinfo.txt contains the output of msinfo32.exe. For information on this output, see your Microsoft documentation.
File system report	FileSystemReport.txt	This file records changes made by the user to the file system. It consists of the following sections: • **Files Relocated** — the files in Layer 0 that were moved by the user to the vDisk. Layer 0 files are those that were inherited from the master image by the machine to which the Personal vDisk is attached. • **Files Removed** — the files in Layer 0 that were hidden by a user's action (for example, removing an application). • **Files Added (MOF,INF,SYS)** — the files with .mof, .inf, or .sys extensions that the user added to the vDisk (for example, when they installed an application such as Visual Studio 2010 that registers a .mof file for autorecovery). • **Files Added Other** — Other files that the user added to the vDisk (for example, when they installed an application). • **Base Files Modified But Not Relocated** — the files in Layer 0 that the user modified but that the Personal vDisk Kernel-Mode drivers did not capture in the vDisk.

Configuration Logging

May 02, 2014

Configuration Logging captures Site configuration changes and administrative activities to the Database. You can use the logged content to:

- Diagnose and troubleshoot problems after configuration changes are made; the log provides a breadcrumb trail
- Assist change management and track configurations
- Report administration activity

You set Configuration Logging preferences, display configuration logs, and generate HTML and CSV reports from Citrix Studio. You can filter configuration log displays by date ranges and by full text search results. Mandatory logging, when enabled, prevents configuration changes from being made unless they can be logged. With appropriate permission, you can delete entries from the configuration log. You cannot use the Configuration Logging feature to edit log content.

Configuration Logging uses a PowerShell 2.0 SDK and the Configuration Logging Service. The Configuration Logging Service runs on every Controller in the Site; if one Controller fails, the service on another Controller automatically handles logging requests.

By default, the Configuration Logging feature is enabled, and uses the Database that is created when you create the Site (the Site Configuration Database). Citrix strongly recommends that you you change the location of the database used for Configuration Logging as soon as possible after creating a Site. The Configuration Logging Database supports the same high availability features as the Site Configuration Database.

Access to Configuration Logging is controlled through Delegated Administration, with the Edit Logging Preferences and View Configuration Logs permissions.

Configuration logs are localized when they are created. For example, a log created in English will be read in English, regardless of the locale of the reader.

Configuration changes and administrative activities initiated from Studio, Director, and PowerShell scripts are logged. Examples of logged configuration changes include working with (creating, editing, deleting assigning):

- Machine Catalogs
- Delivery Groups (including changing power management settings)
- Administrator roles and scopes
- Host resources and connections
- Citrix policies through Studio

Examples of logged administrative changes include:

- Power management of a virtual machine or a user desktop
- Studio or Director sending a message to a user

The following operations are not logged:

- Autonomic operations such as pool management power-on of virtual machines.
- Policy actions implemented through the Group Policy Management Console (GPMC); use Microsoft tools to view logs of those actions.
- Changes made through the registry, direct access of the Database, or from sources other than Studio, Director, or PowerShell.

- When the deployment is initialized, Configuration Logging becomes available when the first Configuration Logging Service instance registers with the Configuration Service. Therefore, the very early stages of configuration are not logged (for example, when the Database schema is obtained and applied, when a hypervisor is initialized).

Manage Configuration Logging

Mar 24, 2015

By default, Configuration Logging uses the database that is created when you create a Site (also known as the Site Configuration Database). Citrix recommends that you change the location of the database used for Configuration Logging (and the database used for the Monitoring Service, which also uses the Site Configuration Database by default) after creating a Site, for the following reasons:

- The backup strategy for the Configuration Logging Database is likely to differ from the backup strategy for the Site Configuration Database.
- The volume of data collected for Configuration Logging (and the Monitoring Service) could adversely affect the space available to the Site Configuration database.
- It splits the single point of failure for the three databases.

Note: Product editions that do not support Configuration Logging do not have a Logging node in Studio. For more information, see XenDesktop 7.6 and XenApp 7.6 Features and Entitlements.

Enable and disable Configuration Logging and mandatory logging

By default, Configuration Logging is enabled, and mandatory logging is disabled.

1. Select Logging in the Studio navigation pane.
2. Select Preferences in the Actions pane. The Configuration Logging dialog box contains database information and indicates whether Configuration Logging and mandatory logging are enabled or disabled.
   - To enable Configuration Logging, select the Enable logging radio button. This is the default setting. If the database cannot be written to, the logging information is discarded, but the operation continues.
   - To disable Configuration Logging, select the Disable logging radio button. If logging was previously enabled, existing logs remain readable with the PowerShell SDK.
   - To enable mandatory logging, clear the Allow changes when the database is disconnected checkbox. No configuration change or administrative activity that would normally be logged will be allowed unless it can be written in the database used for Configuration Logging.
     You can enable mandatory logging only when Configuration Logging is enabled, that is, when the Enable Configuration Logging radio button is selected. If the Configuration Logging Service fails, and high availability is not in use, mandatory logging is assumed. In such cases, operations that would normally be logged are not performed.
   - To disable mandatory logging, select the Allow changes when the database is disconnected check box. Configuration changes and administrative activities are allowed, even if the database used for Configuration Logging cannot be accessed. This is the default setting.

Change the Configuration Logging database location

Note: You cannot change the database location when mandatory logging is enabled, because the location change includes a brief disconnect interval that cannot be logged.

1. Create a database server, using a supported SQL Server version.
2. Select Logging in the Studio navigation pane.
3. Select Preferences in the Actions pane.
4. In the Logging Preferences dialog box, select Change logging database.
5. In the Change Logging Database dialog box, specify the location of the server containing the new database server (using one of the forms in the following table) and the database name.

Database type	What to enter	With this database configuration
Standalone or mirror	servername	The default instance is used and SQL Server uses the default port.
	servername\INSTANCENAME	A named instance is used and SQL Server uses the default port.
	servername,port-number	The default instance is used and SQL Server uses a custom port. (The comma is required.)
Other	cluster-name	A clustered database.
	availability-group-listener	An Always-On database.

- To allow Studio to create the database, click OK. When prompted, click OK, and the database will be created automatically. Studio attempts to access the database using the current Studio user's credentials; if that fails, you are prompted for the database user's credentials. Studio then uploads the database schema to the database. (The credentials are retained only during database creation.)
- To create the database manually, click Generate database script. The generated script includes instructions for manually creating the database. Ensure that the database is empty and that at least one user has permission to access and change the database before uploading the schema.

The Configuration Logging data in the previous database is not imported to the new database. Logs cannot be aggregated from both databases when retrieving logs. The first log entry in the new Configuration Logging database will indicate that a database change occurred, but it does not identify the previous database.

Display configuration log content

When initiating configuration changes and administrative activities, the high level operations created by Studio and Director are displayed in the upper middle pane in Studio. A high level operation results in one or more service and SDK calls, which are low level operations. When you select a high level operation in the upper middle pane, the lower middle pane displays the low level operations.

If an operation fails before completion, the log operation might not be completed in the Database; for example, a start record will have no corresponding stop record. In such cases, the log indicates that there is missing information. When you display logs based on time ranges, incomplete logs are shown if the data in the logs matches the criteria. For example, if all logs for the last five days are requested and a log exists with a start time in the last five days but has no end time, it is included.

When using a script that calls PowerShell cmdlets, if you create a low level operation without specifying a parent high level operation, Configuration Logging will create a surrogate high level operation.

To display configuration log content, select Logging in the Studio navigation pane. By default, the display in the center pane lists the log content chronologically (newest entries first), separated by date.

To filter the display by	Complete this action
Search results	Enter text in the Search box at the top of the middle pane. The filtered display includes the number of search results. To return to the standard logging display, clear the text in the Search box.
Column heading	Click a column heading to sort the display by that field.
A date range	Select an interval from the drop down list box next to the Search box at the top of the middle pane.

Generate reports

You can generate CSV and HTML reports containing configuration log data.

- The CSV report contains all the logging data from a specified time interval. The hierarchical data in the database is flattened into a single CSV table. No aspect of the data has precedence in the file. No formatting is used and no human readability is assumed. The file (named MyReport) simply contains the data in a universally consumable format. CSV files are often used for archiving data or as a data source for a reporting or data manipulation tool such as Microsoft Excel.
- The HTML report provides a human-readable form of the logging data for a specified time interval. It provides a structured, navigable view for reviewing changes. An HTML report comprises two files, named Summary and Details. Summary lists high level operations: when each operation occurred, by whom, and the outcome. Clicking a Details link next to each operation takes you to the low level operations in the Details file, which provides additional information.

To generate a configuration log report, select Logging in the Studio navigation pane, and then select Create custom report in the Actions pane.

- Select the date range for the report.
- Select the report format: CSV, HTML, or both.
- Browse to the location where the report should be saved.

Delete configuration log content

To delete the configuration log, you must have certain Delegated Administration and SQL Server database permissions.

- **Delegated Administration** — You must have a Delegated Administration role that allows the deployment configuration to be read. The built-in Full administrator role has this permission. A custom role must have Read Only or Manage selected in the Other permissions category.
  To create a backup of the configuration logging data before deleting it, the custom role must also have Read Only or Manage selected in the Logging Permissions category.

- **SQL Server database** — You must have a SQL server login with permission to delete records from the database. There are two ways to do this:
  - Use a SQL Server database login with a sysadmin server role, which allows you to perform any activity on the database server. Alternatively, the serveradmin or setupadmin server roles allow you to perform deletion operations.
  - If your deployment requires additional security, use a non-sysadmin database login mapped to a database user who has permission to delete records from the database.
    1. In SQL Server Management Studio, create a SQL Server login with a server role other than 'sysadmin.'
    2. Map the login to a user in the database; SQL Server automatically creates a user in the database with the same name as the login.

3. In Database role membership, specify at least one of the role members for the database user: ConfigurationLoggingSchema_ROLE or dbowner.

   For more information, see the SQL Server Management Studio documentation.

To delete the configuration logs:

1. Select Logging in the Studio navigation pane.
2. Select Delete logs in the Actions pane.
3. You are asked if you want to create a backup of the logs before they are deleted. If you choose to create a backup, browse to the location where the backup archive should be saved. The backup is created as a CSV file.

After the configuration logs are cleared, the log deletion is the first activity posted to the empty log. That entry provides details about who deleted the logs, and when.

Monitor Service OData API

Sep 29, 2014

In addition to using the Citrix Director console to display historical data, you can query data using the Monitor Service's API. You can use the API to:

- Analyze historical trends for future planning
- Perform detailed troubleshooting of connection and machine failures
- Extract information for feeding into other tools and processes; for example, using Microsoft Excel's PowerPivot tables to display the data in different ways
- Build a custom user interface on top of the data that the API provides

The Monitor Service API uses the Open Data (OData) protocol, which is a Web protocol for querying and updating data, built upon Web technologies such as HTTP. For more information about the OData protocol, see: http://www.odata.org.

The Monitor Service API is built on top of SQL Server databases using Windows Communication Foundation (WCF) Data Services that are populated during processing and consolidation. Two endpoints are exposed using WCF with wsHttpBinding. The base address is: http:// {dc-host}/Citrix/Monitor/OData/v2. You can also use SSL to secure endpoints; see Securing endpoints using SSL for more information.

1. The Data endpoint exposes read-only access directly to the database entities and can be accessed using the OData query language. This endpoint allows highly flexible access in terms of filtering and column selection. The Data API URI is: http://{dc-host}/Citrix/Monitor/OData/v2/Data. For more information about accessing the Monitor Service data, see Accessing data using the API.
2. The Methods endpoint exposes service operations that are used by Citrix Director to retrieve data that requires complex grouping and high performance standards, such as queries on the Dashboard and Trends pages. The Methods API URI is: http://{dc-host}/Citrix/Monitor/OData/v2/Methods. Methods are used only in Director itself so are not used by the majority of Citrix customers. They are therefore not documented here.

What's new in this release?

The version of the API included with XenApp and XenDesktop 7.6 provides the following new features:

- **Hotfix inventory.** Using the User Details view or Machine view in Director, you can see a list of all the Citrix hotfixes that have been installed on a machine. You can use the API to extract this data and create custom reports (for example, the state of installed hotfixes over an entire site) or pull it into an analytics engine. New classes have been introduced and the Machine class has been extended to support tracking Citrix hotfixes installed on the controller and VDAs.
- **Anonymous session troubleshooting.** Sessions can be run as a set of pooled local user accounts. The API has a new IsAnonymous property for the Session class (default value FALSE).
- **Hosted application usage reporting.** Director provides new capacity reports that show the usage of hosted applications over time. The API allows you to report on the details of each application instance running in a user session.

All the updates to data are fully documented in the API Reference at http://support.citrix.com/help/monitorserviceapi/7.6/.

The GetSessionSummary method has been deprecated at this release.

Accessing data using the API

Sep 29, 2014

The following types of data are available through the Monitor Service API:

- Data relating to connection failures
- Machines in a failure state
- Session usage
- Logon duration
- Load balancing data
- Hotfixes applied to a machine
- Hosted application usage

For a full description of the data objects, see http://blogs.citrix.com/2013/08/27/xendesktop-7-monitor-service-what-data-is-available/.

To use the Monitor Service OData API, you must be a XenApp or XenDesktop administrator. To call the API, you require read-only privileges; however, the data returned is determined by XenApp or XenDesktop administrator roles and permissions. For example, Delivery Group Administrators can call the Monitor Service API but the data they can obtain is controlled by Delivery Group access set up using Citrix Studio. For more information about XenApp or XenDesktop administrator roles and permissions, see Delegated Administration.

Querying the data

The Monitor Service API is a REST-based API that can be accessed using an OData consumer. OData consumers are applications that consume data exposed using the OData protocol. OData consumers vary in sophistication from simple web browsers to custom applications that can take advantage of all the features of the OData Protocol. For more information about OData consumers, see: http://www.odata.org/ecosystem#consumers.

Every part of the Monitor Service data model is accessible and can be filtered on the URL. OData provides a query language in the URL format you can use to retrieve entries from a service. For more information, see: http://msdn.microsoft.com/en-us/library/ff478141.aspx

The query is processed on the server side and can be filtered further using the OData protocol on the client side.

The data modeled falls into three categories: aggregate data (the summary tables), current state of objects (machines, sessions, etc), and log data, which is really historical events (connections, for example).

Note: Enums are not supported in the OData protocol; integers are used in their place. To determine the values returned by the Monitor Service OData API, see http://support.citrix.com/help/monitorserviceapi/7.6/.

Aggregation of data values

The Monitor Service collects a variety of data, including user session usage, user logon performance details, session load balancing details, and connection and machine failure information. Data is aggregated differently depending on its category. Understanding the aggregation of data values presented using the OData Method APIs is critical to interpreting the data. For example:

- Connected Sessions and Machine Failures occur over a period of time, therefore they are exposed as maximums over a time period.

- LogOn Duration is a measure of length of time, therefore is exposed as an average over a time period.
- LogOn Count and Connection Failures are counts of occurrences over a period of time, therefore are exposed as sums over a time period.

Concurrent data evaluation

Sessions must be overlapping to be considered concurrent. However, when the time interval is 1 minute, all sessions in that minute (whether or not they overlap) are considered concurrent: the size of the interval is so small that the performance overhead involved in calculating the precision is not worth the value added. If the sessions occur in the same hour, but not in the same minute, they are not considered to overlap.

Correlation of summary tables with raw data

The data model represents metrics in two different ways.:
- The summary tables represent aggregate views of the metrics in per minute, hour, and day time granularities.
- The raw data represents individual events or current state tracked in the session, connection, application and other objects.

When attempting to correlate data across API calls or within the data model itself, it is important to understand the following concepts and limitations:

- **No summary data for partial intervals.** Metrics summaries are designed to meet the needs of historical trends over long periods of time. These metrics are aggregated into the summary table for complete intervals. There will be no summary data for a partial interval at the beginning (oldest available data) of the data collection nor at the end. When viewing aggregations of a day (Interval=1440), this means that the first and most recent incomplete days will have no data. Although raw data may exist for those partial intervals, it will never be summarized. You can determine the earliest and latest aggregate interval for a particular data granularity by pulling the min and max SummaryDate from a particular summary table. The SummaryDate column represents the start of the interval. The Granularity column represents the length of the interval for the aggregate data.
- **Correlating by time.** Metrics are aggregated into the summary table for complete intervals as described above. They can be used for historical trends, but raw events may be more current in the state than what has been summarized for trend analysis. Any time-based comparison of summary to raw data needs to take into account that there will be no summary data for partial intervals that may occur or for the beginning and ending of the time period.
- **Missed and latent events.** Metrics that are aggregated into the summary table may be slightly inaccurate if events are missed or latent to the aggregation period. Although the Monitor Service attempts to maintain an accurate current state, it does not go back in time to recompute aggregation in the summary tables for missed or latent events.
- **Connection High Availability.** During connection HA there will be gaps in the summary data counts of current connections, but the session instances will still be running in the raw data.
- **Data retention periods.** Data in the summary tables is retained on a different grooming schedule from the schedule for raw event data. Data may be missing because it has been groomed away from summary or raw tables. Retention periods may also differ for different granularities of summary data. Lower granularity data (minutes) is groomed more quickly than higher granularity data (days). If data is missing from one granularity due to grooming, it may be found in a higher granularity. Since the API calls only return the specific granularity requested, receiving no data for one granularity does not mean the data doesn't exist for a higher granularity for the same time period.
- **Time zones.** Metrics are stored with UTC time stamps. Summary tables are aggregated on hourly time zone boundaries. For time zones that don't fall on hourly boundaries, there may be some discrepancy as to where data is aggregated.

Data granularity and retention

The granularity of aggregated data retrieved by Director is a function of the time (T) span requested. The rules are as follows:

- 0 < T <= 1 hour uses per-minute granularity
- 0 < T <= 30 days uses per-hour granularity
- T > 31 days uses per-day granularity

Requested data that does not come from aggregated data comes from the raw Session and Connection information. This data tends to grow fast, and therefore has its own grooming setting. Grooming ensures that only relevant data is kept long term. This ensures better performance while maintaining the granularity required for reporting. For customers who are not licensed to use the Platinum edition, grooming begins at day 8 regardless of the default grooming retention. Platinum customers can change the grooming retention to their desired number of retention days, otherwise the default is used.

The following settings are used to control grooming:

Setting name	Affected grooming	Default value (days)	Accessed using
GroomSessionsRetentionDays	Session and SessionDetail records	7 for non-Platinum users, 90 for Platinum	Cmdlet (set/get-monitorconfiguration)
GroomSummariesRetentionDays	DesktopGroupSummary, FailureLogSummary and LoadIndexSummary records. Aggregated data - daily granularity.	7 for non-Platinum users, 90 for Platinum	Cmdlet (set/get-monitorconfiguration)
GroomHourlyRetentionDays	Aggregated data - hourly granularity	32 days	Monitor.Configuration Database Table. See note below.
GroomMinuteRetentionDays	Aggregated data - minute granularity	3 days	Monitor.Configuration Database Table. See note below.
GroomFailuresRetentionDays	MachineFailureLog and ConnectionFailureLog records	7 for non-Platinum users, 90 for Platinum	Cmdlet (set/get-monitorconfiguration)
GroomLoadIndexesRetentionDays	LoadIndex records	7 for non-	Cmdlet (set/get-monitorconfiguration)

Setting name	Affected grooming	Default value (days)	Accessed using
GroomDeletedRetentionDays	Machine, Catalog, DesktopGroup and Hypervisor entities that have a LifecycleState of 'Deleted'. This will also delete any related Session, SessionDetail, Summary, Failure or LoadIndex records.	7 for non-Platinum users, 90 for Platinum	Cmdlet (set/get-monitorconfiguration)
GroomMachineHotfixHistoryRetentionDays	Hotfixes applied to the VDA and Controller machines	90 for both non-Platinum and Platinum users	Cmdlet (set/get-monitorconfiguration)

Caution: Modifying values on the Monitor Service database requires restarting the service for the new values to take effect. You are advised to make changes to the Monitor Service database only under the direction of Citrix Support. Retaining data for long periods will have the following implications on table sizes:

- **Hourly data.** If hourly data is allowed to stay in the database for up to two years, a site of 1000 delivery groups could cause the database to grow as follows:
  1000 delivery groups x 24 hours/day x 365 days/year x 2 years = 17,520,000 rows of data. The performance impact of such a large amount of data in the aggregation tables is significant. Given that the dashboard data is drawn from this table, the requirements on the database server may be large. Excessively large amounts of data may have a dramatic impact on performance.

- **Session and event data.** This is the data that is collected every time a session is started and a connection/reconnection is made. For a large site (100K users), this data will grow very fast. For example, two years worth of these tables would gather more than a TB of data, requiring a high-end enterprise-level database.

Securing endpoints using SSL

Apr 27, 2015

This document explains how to use SSL to secure the Monitor Service OData API endpoints. If you choose to use SSL, you must configure SSL on all Delivery Controllers in the site; you cannot use a mixture of SSL and non-SSL.

To secure Monitor Service endpoints using SSL, you must perform the following configuration. Some steps need to be done only once per site, others must be run from every machine hosting the Monitor Service in the site. The steps are described below.

Part 1: Certificate registration with the system

1. Create a certificate using a trusted certificate manager. The certificate must be associated with the port on the machine that you wish to use for OData SSL.
2. Configure the Monitor Service to use this port for SSL communication. The steps depend on your environment and how this works with certificates. The following example shows how to configure port 449:

- Associate the certificate with a port:
  netsh http add sslcert ipport=0.0.0.0:449 certhash=97bb629e50d556c80528f4991721ad4f28fb74e9 appid='{00000000-0000-0000-0000-000000000000}'
  Tip: In a PowerShell command window, ensure you put single quotes around the GUID in the appID, as shown above, or the command will not work. Note that a line break has been added to this example for readability only.

Part 2: Modify the Monitor Service configuration settings

1. From any Delivery Controller in the site, run the following PowerShell commands once. This removes the Monitor Service registration with the Configuration Service.

```
asnp citrix.*

$serviceGroup = get-configregisteredserviceinstance -servicetype Monitor | Select -First 1 ServiceGroupUid

remove-configserviceGroup -ServiceGroupUid $serviceGroup.ServiceGroupUid
```

2. Do the following on all Controllers in the site:
   - Using a cmd prompt, locate the installed Citrix Monitor directory (typically in C:\Program Files\Citrix\Monitor\Service). Within that directory run:
     Citrix.Monitor.Exe -CONFIGUREFIREWALL -ODataPort 449 -RequireODataSsl
   - Run the following PowerShell commands:

```
asnp citrix.*  (if not already run within this window)

get-MonitorServiceInstance | register-ConfigServiceInstance

Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-MonitorServiceGroupMembership
```

Examples

Sep 24, 2014

The following examples show how to export Monitor Service data using the OData API.

Example 1 - Raw XML

1. Place the URL for each data set into a web browser that is running with the appropriate administrative permissions for the XenApp or XenDesktop Site. Citrix recommends using the Chrome browser with the Advanced Rest Client add-in.
2. View the source.

Example 2 - PowerPivot with Excel

These instructions assume that you have already installed Microsoft Excel and PowerPivot.

Open Excel (running with the appropriate administrative permissions for the XenApp or XenDesktop Site).

If you are using Excel 2010:

1. Click the PowerPivot tab.
2. Click PowerPivot Window.
3. Click **From Data Feeds** in the ribbon.
4. Choose a Friendly Connection Name (for example: XenDesktop Monitoring Data) and enter the data feed url: http://{dc-host}/Citrix/Monitor/OData/v2/Data (or https: if you are using SSL).
5. Click **Next**.
6. Select the tables you want to import into Excel and click **Finish**. The data is retrieved.
7. You can now use PowerPivot to view and analyze the data with PivotTables and PivotCharts. For more information, see the Learning Center: http://www.microsoft.com/en-us/bi/LearningCenter.aspx

If you are using Excel 2013:

1. Click the Data tab.
2. Choose From Other Sources > From OData Data Feed
3. Enter the data feed url: http://{dc-host}/Citrix/Monitor/OData/v1/Data (or https: if you are using SSL) and click **Next**.
4. Select the tables you want to import into Excel and click **Next**.
5. Accept name defaults or customize names and click **Finish**.
6. Choose **Connection Only** or **Pivot Report**. The data is retrieved.
7. You can now use PowerPivot to view and analyze the data with PivotTables and PivotCharts. For more information, see the Learning Center: http://www.microsoft.com/en-us/bi/LearningCenter.aspx

Example 3 - LINQPad

These instructions assume that you have already installed LINQPad.

1. Run LinqPad with the appropriate administrative permissions for the XenApp or XenDesktop Site.
   Tip: the easiest way is to download, install and run on the Delivery Controller.
2. Click the Add connection link.
3. Choose WCF Data Services 5.1 (OData 3) and click **Next**.
4. Enter the data feed URL: http://{dc-host}/Citrix/Monitor/OData/v2/Data (or https: if you are using SSL). If necessary, enter the username and password to access the Delivery Controller. Click **OK**.

5. You can now run LINQ queries against the data feed and export the data as needed. For example, right-click Catalogs and choose **Catalogs.Take(100)**. This returns the first 100 Catalogs in the database. Choose Export>Export to Excel with formatting.

For further worked examples of how to use the API with LINQPad, see http://blogs.citrix.com/2014/01/14/creating-director-custom-reports-for-monitoring-xendesktop/.

XenApp and XenDesktop SDK

Apr 28, 2015

XenApp and XenDesktop provide an SDK based on a number of Microsoft Windows PowerShell version 3.0 snap-ins that allows you to perform the same tasks as you would with the Citrix Studio console, together with tasks you cannot do with Studio alone.

As from version 7.5, XenApp and XenDesktop share a unified architecture and management: the FlexCast Management Architecture. This means that XenApp provides many features previously only available in XenDesktop; elements of the SDK that relate to common features therefore apply equally to both XenApp and XenDesktop, even though the commands themselves refer only to XenDesktop.

Key differences between the XenDesktop 5 and XenDesktop 7 SDK

- **New high-level SDK** — XenDesktop 7 provides a new high-level SDK that enables you to script and automate site creation and maintenance quickly and easily. The high-level SDK insulates you from much of the complexity of the low-level SDKs, such that you can create a new site simply by running two cmdlets.
- **New low-level SDKs** — Individual low-level SDKs are provided for the new XenDesktop 7 services, including a dedicated and enhanced SDK for the Delegated Administration Service (DAS), which was previously part of the Broker SDK in XenDesktop 5. There are also SDKs for new features including the Monitor Service, Environment Test, and Configuration Logging.
- **Windows Server OS Machine catalogs and delivery groups** — You can use the XenDesktop 7 SDK to deliver cost-effective applications and desktops hosted on server operating systems.
- **Desktop OS Machine applications** — Desktop OS Machine applications have changed significantly at the SDK level. If you have existing scripts for running applications on Desktop OSs, you will have to update these scripts for XenDesktop 7 as there is little backwards compatibility.
- **Apply settings to machines in Delivery Groups** — In XenDesktop 7, using configuration slots, you can apply settings to machines in a specific delivery group, rather than to all machines in a site. This enables you to configure, for a given delivery group, which settings apply to that group. A number of pre-defined configuration slots are provided that contain different types of settings, such as settings for StoreFront addresses for use with Receiver or App-V publishing server locations. You can use one collection of settings from a slot to affect only a particular delivery group, and a different collection of settings from the same slot to affect another delivery group. You can use names appropriate to your particular deployment; for example, "Sales Department policy."
- **Catalog types replaced** — In XenDesktop 7, catalog types have been replaced by catalogs with individual properties. However, for backwards compatibility, you can still use existing scripts that employ catalog types, such as single image (pooled) and thin clone (dedicated) etc., but internally these are converted into sets of properties.
  Caution: Backwards compatibility with XenDesktop 5 catalog types has been maintained where possible and practicable. However, when writing new scripts, do not use catalog types; instead, specify catalogs with individual properties.
- **Desktop object replaced** — In XenDesktop 5, the Desktop object is one of the main types of SDK object used in Broker SDK scripts. The Desktop object describes both the machine and the session on the machine. In XenDesktop 7, this object is replaced by the Session object and the Machine object, both of which have been expanded to do the work of the Desktop object. However, for backwards compatibility, you can still use existing scripts that employ the Desktop object.
  Caution: Backwards compatibility with XenDesktop 5 has been maintained where possible and practicable. However, when writing new scripts, do not use the Desktop object; instead, specify Session and Machine objects.

Differences in policy rules

There are differences between the SDK and the Studio console in terms of policy rules. Entitlement and assignment policy rules are independent entities in the SDK; in the console, these entities are not visible as they are seamlessly merged with the Delivery Group. Also, access policy rules are less restrictive in the SDK.

Use the SDK

The SDK comprises of a number of PowerShell snap-ins installed automatically by the installation wizard when you install the Controller or Studio components.

To access and run the cmdlets:

1. Start a shell in PowerShell 3.0.
   To start a shell from the console, click **Studio**, select the PowerShell tab, and click on **Launch PowerShell**.

   You must run the shell or script using an identity that has Citrix administration rights. Although members of the local administrators group on the Controller automatically have full administrative privileges to allow XenDesktop to be installed, Citrix recommends that for normal operation, you create Citrix administrators with the appropriate rights, rather than use the local administrators account. If you are running Windows Server 2008, you must run the shell or script as a Citrix administrator, and not as a member of the local administrators group.

2. To use SDK cmdlets within scripts, set the execution policy in PowerShell.
   For more information about PowerShell execution policy, see your Microsoft documentation.

3. Add the snap-ins you require into the PowerShell environment using the **Add -PSSnapin** command in the Windows PowerShell console. V1 and V2 denote the version of the snap-in (XenDesktop 5 snap-ins are version 1; XenDesktop 7 snap-ins are version 2.). For example, type:
   `Add-PSSnapin Citrix.ADIdentity.Admin.V2`
   To import all the cmdlets, type:

   `Add-PSSnapin Citrix.*.Admin.V*`
   After importing, you have access to the cmdlets and their associated help.

For an example of a typical use case, see Get started with the SDK.

Tip: For a complete listing of all help text for the cmdlets, see PowerShell cmdlet help.

Group Policy SDK usage

The Citrix Group Policy SDK allows you to display and configure Group Policy settings and filters. It uses a PowerShell provider to create a virtual drive that corresponds to the machine and user settings and filters. The provider appears as an extension to New-PSDrive. To use the Group Policy SDK, either Studio or the XenApp and XenDesktop SDK must be installed.

Adding the Group Policy SDK

1. To add the Group Policy SDK, type:
   `Add-PSSnapin citrix.common.grouppolicy`
2. To access help, type:
   `help New-PSDrive -path localgpo:/`

Using the Group Policy SDK

1. To create a virtual drive and load it with settings, type:

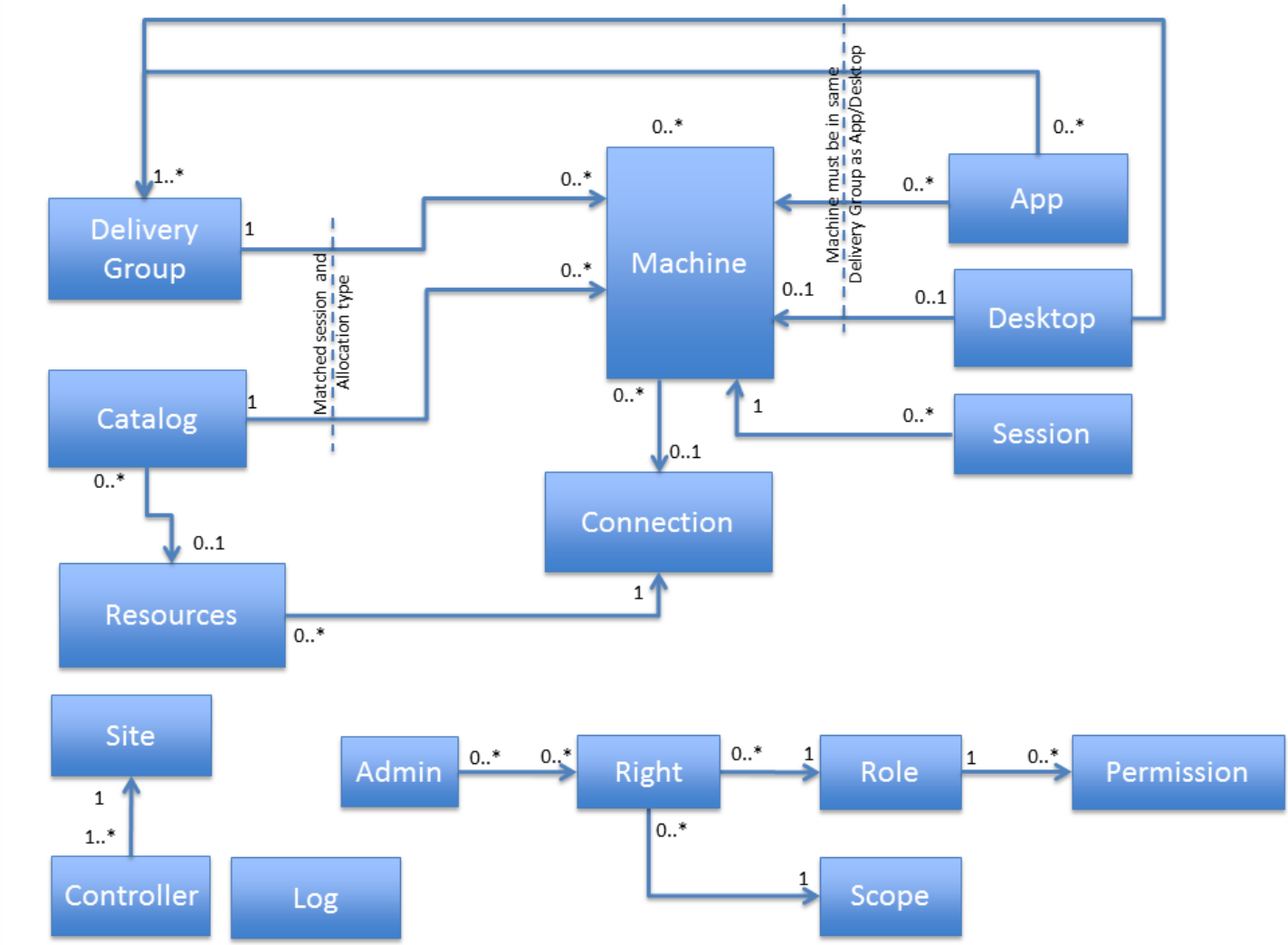
New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy
— -Controller
<string>
New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy
— -Controller
<string>

where
— -Controller
is the fully qualified domain name of a controller in the site you want to connect to and load settings from.

Understanding the XenDesktop Administration Model

Apr 27, 2015

XenDesktop 7 has an administration model that is defined by a set of objects and their interconnections, as shown in the following illustration.



The following sections describe each object, its responsibilities, characteristics and basic properties.

Connection

A Connection entity provides the details required to establish a connection to the administration point for a virtualization platform. These details are used to provide any power management and provisioning functions that are required. The Connection defines:

- The identity of the connection, which includes a name and an internal ID value (a GUID).
- Type—XenServer, SCVMM or vCenter.
- Username—the account name to use for connections to the hypervisor.
- Password—the password to use for connections to the hypervisor.
- The state of the connection and whether the hypervisor can be communicated with or not.
- Any current alerts raised by the hypervisor.

The password cannot be read back once set and is stored in the database in an encrypted form.

There is one of these entities in the model for each platform definition; however, there will be many connections established to the virtualization platform at run time to service the requirements of the XenDesktop deployment. These connections can be shared by many Resources entities (see below for further details).

Note: When setting up a Connection with XenServer, you specify a host or XenServer pool; when setting up a Connection with Microsoft Hyper-V or VMware, you provide details to the management servers (SCVMM or vCenter). Also, when configuring a Connection, you must specify the user name in the correct format, depending on the virtualization solution you're using. If you're setting up a Connection with XenServer, specify a plain user name; for example "username"; for a Connection with VMware or Hyper-V, specify a domain user name; for example "domain\username".

Resources

Note: This applies only to the creation of new machines when using Machine Creation Services (MCS) or Provisioning Services (PVS).

This setting defines a set of resources within the virtualization platform that are available for the product to consume. This allows the administrator to constrain deployment to a subset of the resources that the platform provides, and enables differing sets of resources to be defined for different purposes. This can control the storage and networking usage of machines provisioned within the site. The Resources entity defines:

- Networks—the networks which are able to be used when provisioning new machines into the virtualization plaform (for PVS, this is the streaming network; only one can be chosen or the first one is used).
- Storage—the storage to use when provisioning new machines into the virtualization platform.

At least one Resources setting must be defined for each Connection object if a provisioning mechanism is to be used. Many Resources settings can be linked to a single Connection.

The connection details are provided by the Connection entity.

Note: When specifying Resources on a Connection to either SCVMM or vCenter, you select the host or cluster as well as the storage and networking.

Administrator

This defines the person who can administer the product. There can be various administrators of the product, each with a different set of capabilities within the product. The Administrator defines:

- The AD account the administrator is defined by, defined as their name and SID value. This can be an individual user or a security group.
- The rights the administrator has (i.e. what roles are available over which scopes).

Machine

A machine is a representation of a virtual or physical computer that can be used within a site to provide sessions to users. The machine defines:

- Identity of the machine, such as SAM name, DNS name, host (hypervisor) name, IP address, SID, License ID etc.
- Status of the machine, including power state, registration state, Personal vDisk state, load index etc. A summary state value aggregates many of these into a single state value.
- Information about the environment and configuration of the machine, such as version numbers of installed operating systems and Citrix components, including the 'functional level' of the machine.
- Data relating to the most recent activity of the machines, such as the last reason for de-registering, the last power action performed on the machine, the last connection failure etc.

- Maintenance mode and 'WindowsConnectionSetting' states for controlling the enable/disable/drain behavior of the machine.
- Visible user-resource settings for the machine for the assigned desktop case, such as icon, published name etc.
- For multi-session machines (Server OS Machines), aggregate information about the sessions running, such as the number of sessions active, pending etc.
- 'Tag' values associated with an assigned machine.
- Provisioning image information, such as the path to the master image, the provisioning scheme used to create the machine, and whether or not the machine has an updated image pending on its next reboot.

Most of the machine values are exposed by the Broker Service SDK, but items are also exposed by other services, such as the Machine Creation Service (MCS). Other values shown on a per-machine basis are inherited from the Catalog or Delivery Group (if any) that the machine is associated with, or from the provisioning scheme used to create it. For example, the machine type which is defined at the Catalog level by a combination of factors such Physical or Virtual, static or random, how user changes are persisted and others. For single-session machines (Desktop OS Machines), information about the session (if any) that is running on the machine is also associated with the machine. This includes connected user identity, session state, protocol in-use and so on. Machines can exist only in the model if they are defined as part of a Catalog; they cannot exist outside of this concept.

Catalog

A Catalog defines a set of machines that are usually, but not always, expected to be equivalent. Multiple Catalogs can exist within a single deployment, enabling different sets of machines to be built and stored for different purposes. The Catalog defines:

- Catalog type, defined by the values of the following properties:
  1. The provisioning method for the machines (MCS, PVS or manual)
  2. How machines in the Catalog are allocated to users: statically with permanent assignment to users or randomly each time a user requests a resource
  3. Whether the machines are single-session (Desktop OS Machines) or multi-session (Server OS Machines)
  4. Whether the machines are physical or virtual
  5. How user changes to machines are handled, whether they are discarded after the user logs off or preserved locally on the machine or using Personal vDisk
- If the Catalog is to be used for Remote PC users and, if so, which Active Directory (AD) OUs are to be associated with the Catalog, and which Delivery Groups are associated with the Catalog.
- MCS provisioning-associated details (if MCS provisioning is to be used):
  1. Master image for the machines
  2. Memory size and number of CPUs
  3. Personal vDisk disk size, drive letter, and allocation percentages
  4. AD account naming scheme and OU where the machines are created, and a list of already created accounts
- Details of any PVS server associated with the Catalog.
- The functional level expected for machines; machines of lower functional level are not allowed to register with the site.

Also exposed at the Catalog level are some usage values for machines consumed or available in the Catalog.

Delivery Group

The Delivery Group provides details about a collection of machines used to provide desktops and/or applications to an end-user. Many Delivery Groups can be linked to the same Catalog, enabling machines in a Catalog to be distributed in various ways depending on the requirements of different user sets. The Delivery Group defines:

- The allocation type of the machines in the group, indicating whether machines are shared between users (random) or

assigned persistently to one or more users (static), and whether the machines are single-session (Desktop OS) or multi-session (Server OS) machines.

- The delivery type of the group, indicating whether the group serves applications only, desktops only, or a mixture of applications and desktops to users.
- Settings controlling the power management of machines in the group, including:
  1. Which hours of the day, on different days of the week, are considered 'peak' time
  2. How many machines to keep running at different hours of the day on different days of the week for random/unassigned machines, including buffer sizes
  3. The timezone to use for evaluating the hours of the day for the above settings
  4. Whether and how assigned machines are power managed
  5. Whether and how to shut down or suspend machines after trigger events, such as user disconnect or logoff
  6. Whether or not the machines are considered corrupted by any sessions run on them and forced to restart to return them back to a clean, known state after each use
- How desktop resources from the group appear to an end-user, including icon used, color depth and name. Also defined is the security level required on the ICA connections for machines in the group. For desktop resources, the number of desktops each user is allowed simultaneously from the group.
- Rules used to establish the availability of these machines to the end users. Rules can factor in, not just the user's identity, but also where the user is connecting from and how, what the state of the client device is, and which remoting protocols are supported.
- Whether the group is enabled or disabled, including setting of maintenance mode.
- Whether the end-user is allowed to reset the machine themselves (for example, using StoreFront).
- 'Tag' values associated with a random/shared group.
- The functional level expected for machines in the group; machines of lower functional level are not allowed to register with the site.
- Whether the group is to be used for Remote PC users, and which Remote PC catalogs are associated with the group.
- A schedule for regularly rebooting multi-session (Server OS) machines at a particular time and day, and settings to control how that reboot is done.

Also associated with Delivery Groups are settings for features such as Profile management and Storefront URL settings, which are separately defined as 'Machine Configuration' objects and associated with one or more Delivery Groups.

Application

This provides details of a seamless (i.e. floating window, separate from a desktop) application that is to be made available to end-users.Typically, each application is associated with a single delivery group, but application definitions can be shared across multiple groups, if required. Applications can be run either on a remote machine and displayed on the local client desktop, or installed and run on the local client machine with windows overlaid onto a remote desktop. The application defines:

- The type of the application, whether 'HostedOnDesktop' or 'InstalledOnClient'.
- For HostedOnDesktop applications:
  1. The path to the application initial executable to be run on the VDA machine and the command line parameters, if any, to be supplied when the application is started
  2. Optionally, a specific set of users who have access to the application as a subset of users who have access to the Delivery Group(s)
  3. Any application-specific settings to be applied to the application process, including a CPU priority level, whether the application should wait for proxy printers to be created or not, etc.
- For InstalledOnClient applications:
  1. A flag to indicate that the icon for the application is to be fetched from the client device

2. A flag to specify that extra security measures are to be taken with the arguments supplied to the application

- How the application resource appears to an end-user, including icon used, folder location on the client device, name and whether the shortcut appears in the start menu, desktop or both.
- Any file-type associations for the application, associating file extensions with the application.
- Which Delivery Group(s) it is associated with, along with an optional priority value for choosing between multiple groups.
- Whether the application is enabled and, separately, whether it is visible to end users or not.

Desktop

In XenDesktop 7, the Desktop object (which describes both the machine and the session on the machine) is replaced by the Session object and the Machine object, both of which have been expanded to do the work of the Desktop object.

Session

This provides details of a Windows session running on a machine controlled by the site. The session may be one initiated by XenDesktop or XenApp, or one that was created by other means, such as a user logging directly onto the machine through the console or over RDP.

The session defines:

- The identity of the machine where the session is running, including machine DNS name, IP address, NetBios name, SID etc.
- The identity of the user who is running the session, including SAM name, UPN, SID, etc.
- The identity of the user who brokered the connection to the session, including SAM name, SID, etc.
- The identity of the endpoint client machine being used to connect to the session, including the device name, IP address, ID.
- The identity of the machine used to request the launch, i.e. the web server from which the launch was made. This includes name and IP address.
- The identity of the machine used to act as a gateway for the session connection, including machine DNS name, IP address.
- Details of significant events in the session, including start time, the time when the session was most recently connected to, brokered to etc.
- The durations of aspects of the most recent session creation or connection, including the time taken to broker the session, time taken to create the session etc.
- The current status of the session, including an overall session state, whether the ICA connection is secured, what protocol is being used.
- The current state of the machine running the session, incuding an overall summary state, power state, etc.
- Details about how the session connection was made, such as whether the session was brokered or connected to autonomously, the session context 'Smart Access' tags in force.
- Whether the session is 'hidden' or not. Sessions can become hidden if certain types of problems are encountered when a user launches an application or desktop.
- The list of brokered applications executing in the session.

The session SDK object also provides information from the related machine, Delivery Group and Catalog SDK objects. This information includes identity information, basic configuration and status information.

Controller

This provides details of the individual Delivery Controller machines in the site. Most of the data is dynamic state data from the running site, rather than configuration settings. The controller shows:

- Which 'site services' are active on each controller.
- The version of the controller components.
- The identity of the controller machine, as fully qualified DNS name, SAM name, SID etc.
- The type and version of the OS of the controller machine.
- Current controller and service status, and most recent activity times.
- Counts of machines registered with the controller.
- Which hypervisor connections are associated with the controller for site service location purposes.

Most of the controller values are exposed from the Broker Service SDK, but other items are exposed from other services, such as the Machine Creation Service.

Site

The Site is a top-level, logical representation of the XenDesktop site, from the perspective of the configuration services running within it. The site contains licensing information, site metadata and the site name, among others.

A XenDesktop installation has only a single configuration site instance. The Site object has the following properties:

- Name
- Controllers—list of controllers in the site
- Databases—list of databases used by the site
- DefaultIconUid
- LicenseInformation
- Metadata

Log

This provides details of the collected configuration logs, which describe the administrator activity on the site since logging was enabled. Administrator read actions are not logged, but any administrator action that changes the configuration or state of the site is included in the log. You can view the log at one of three levels: high-level logs, low-level logs and operation details. Each low-level log is a part of a larger high-level operation which is logged, while operation details describe elements within a single low-level operation. Log items show:

- The identity of the administrator who performed the operation, including the IP address of the machine from which it was performed.
- When the operation took place, both start and end times.
- Whether the operation succeeded or failed for any reason.
- A description of the operation, as a text string and also characterised by operation type, source type, target type etc.
- Details of parameters supplied to the operation.
- Any parent/child relationship in the log hierarchy.
- For changes in configuration, a before and after value for the items changed.

For more information about what is logged, see the Configuration Logging documentation.

Right

This defines a combination of role and the scope over which role permissions are allowed. Permissions defined in the role can be executed by the specified administrator, but only on objects that are directly or indirectly associated with the specified scope. The Right defines:

- The role whose permissions are to be allowed.

- The scope over which the role permissions are to be allowed.

Rights are not SDK objects that can be manipulated separately; they are always associated with a particular Administrator object. A single administrator can have many rights, with the total capability of the administrator being the sum of all their individual rights.

Scope

This defines a named grouping for objects, where objects in the grouping have administrator rights over objects controlled on a role-by-role basis. SDK objects of various types can have scopes directly associated with them, such as Catalogs, Delivery Groups, Connections, Resources etc. These SDK objects have properties that list the scopes that the object has been associated with. Other SDK objects have administrator rights granted by a secondary association with other objects which are directly scoped. For example, Machine objects inherit their scope associations from the Catalogs and Delivery Groups they are members of; Session objects inherit their scope associations from the machines on which the session is running. Some scopes are pre-defined (in practice only the 'All' scope is currently built-in) but you can create other scopes to specify suitable grouping definitions for your particular deployment.

The Scope defines:

- The identity of the scope, which includes a name and an internal ID value (a GUID).
- Whether the scope is built-in or not.

Role

Defines a set of permissions that an administrator can perform. Roles are always granted to administrators with an associated scope; they do not provide rights on their own, although some roles may have general permissions that apply to objects which do not have any scopes associated with them ('unscoped objects'). Some roles are pre-defined, but you can create other custom roles to specify suitable sets of permissions for your particular deployment. A Role defines:

- The identity of the role, which includes a name and an internal ID value (a GUID)
- Whether the role is built-in or not
- The set of permissions that make up the role

The built-in roles are:
- Full Administrator—can perform all tasks and operations.
- Read Only Administrator—can see all objects in specified scopes, as well as global information, but cannot change anything.
- Machine Catalog Administrator—can create and manage Machine Catalogs and provision machines.
- Delivery Group Administrator—can deliver applications, desktops, and machines; can also manage the associated sessions. Allows creation and managing of Delivery Groups and applications.
- Help Desk Administrator—can view Delivery Groups, and manage the sessions and machines associated with those groups. Allows viewing of end-user resources and limited state change actions for troubleshooting end-user problems, but does not allow most configuration changes.
- Host Administrator—can manage host connections and their associated resource settings.

Permission

Defines a single console-level task or operation that is allowed when the permission is included in a role. Each permission can allow several low-level SDK operations (cmdlets), and a particular low-level SDK operation can be granted by any number of related permissions. A Permission defines:

- The identity of the permision, which includes a name and an internal ID value (a GUID).
- The permission group membersip of the permission. Permission groups collect together permissions relating to a particular functional area.
- The set of low-level SDK operations covered by the permission.

Get started with the SDK

Apr 27, 2015

To create a script, perform the following steps:

1. Use Citrix Studio to perform the operation that you want to script; for example, to create a catalog for a set of Machine Creation Services Machines.
2. Collect the log of SDK operations that Studio made to perform the task.
3. Review the script to understand what each part is doing. This will help you with the customization of your own script. For more information, see the example use case which explains in detail what the script is doing.
4. Convert and adapt the Studio script fragment to turn it into a script that is more consumable. To do this:
   - Use variables. Some cmdlets take parameters, such as TaskId. However, it may not be clear where the value used in these parameters comes from because Studio uses values from the result objects from earlier cmdlets.
   - Remove any commands that are not required.
   - Add some steps into a loop so that these can be easily controlled. For example, add machine creation into a loop so that the number of machines being created can be controlled.

Examples

Note: When creating a script, to ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described above rather than copying and pasting the example scripts.

Examples	Description
Create catalog	Script: create a catalog for a set of Machine Creation Services (MCS) machines
Example: Create and configure a host	Script: create and configure a host
Example: Create a PvD Desktop	Script: create a Delivery Group containing Personal vDisk (PvD) desktops
Example: Get load balancing information	Display load index values for Server OS Machines

Example: Create a catalog

Apr 27, 2015

The following example shows how to create a catalog for a set of Machine Creation Services (MCS) machines.

Before you begin, make sure you follow the steps detailed in Get started with the SDK. This document tells you how to use Studio to perform the operation you want to script (in this case, to create a catalog for a set of Machine Creation Services machines) and collect the log of SDK operations that Studio made to perform the task. This output can then be customized to produce a script for automating catalog creation.

Note: To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script. Line numbers and line breaks have been added to the script for readability.

Understand the script

The following section explains what each part of the script produced by Studio is doing. This will help you with the customization of your own script. Line numbers have been added for readability.

```
1. Start-LogHighLevelOperation -AdminAddress 'ddc.dumdev.internal.citrix.com:80'
-Source 'Studio' -StartTime 29/05/2013 14:43:08 -Text 'Create Machine Catalog `''ExampleMachines`''
```

Starts a logged operation and returns a log ID which is supplied to subsequent operations to associate them with the larger task.

```
2. New-BrokerCatalog  -AdminAddress 'ddc.dumdev.internal.citrix.com:80' -AllocationType 'Permanent'
-Description 'Example Machines' -IsRemotePC $False -LoggingId f39a2792-064a-43eb-97c7-397cc1238e46
-MinimumFunctionalLevel 'L7' -Name 'ExampleMachines' -PersistUserChanges 'OnPvd' -ProvisioningType 'MCS'
-Scope @() -SessionSupport 'SingleSession'
```

Creates a Broker catalog. This catalog is populated with machines which are about to be created.

```
3. New-AcctIdentityPool  -AdminAddress 'ddc.dumdev.internal.citrix.com:80' -AllowUnicode
-Domain 'dumdev.internal.citrix.com' -IdentityPoolName 'ExampleMachines'
-LoggingId f39a2792-064a-43eb-97c7-397cc1238e46 -NamingScheme 'Example-####'
-NamingSchemeType 'Numeric' -OU 'OU=DUM VMs,DC=dumdev,DC=internal,DC=citrix,DC=com' -Scope @()
```

Creates an Identity Pool. This defines the mechanism for creating AD computer accounts. This becomes a container for AD accounts created for the machines that are to be created.

```
4. Set-BrokerCatalogMetadata  -AdminAddress 'ddc.dumdev.internal.citrix.com:80' -CatalogId 1
-LoggingId f39a2792-064a-43eb-97c7-397cc1238e46 -Name 'Citrix_DesktopStudio_IdentityPoolUid'
-Value 'b99aee6d-8772-4dbc-978b-8eb9a26e2407'
```

Sets metadata on the Broker catalog with details of the Identity Pool. This is not essential.

```
5. Test-ProvSchemeNameAvailable  -AdminAddress 'ddc.dumdev.internal.citrix.com:80'
-ProvisioningSchemeName @('ExampleMachines')
```

Checks that the requested name is available. This is not essential.

```
6. New-ProvScheme  -AdminAddress 'ddc.dumdev.internal.citrix.com:80' -CleanOnBoot -HostingUnitName 'SharedNFS'
-IdentityPoolName 'ExampleMachines' -LoggingId f39a2792-064a-43eb-97c7-397cc1238e46
-MasterImageVM 'XDHyp:\hostingunits\SharedNFS\BaseVM.vm\Base OS, domain joined and activated.snapshot
\Pre-reqs installed.snapshot\Updates Applied.snapshot\VDA75-no agent.snapshot\Updated Agent.snapshot'
-NetworkMapping @{0='xdhyp:\hostingunits\SharedNFS\Network 0.network'} -PersonalVDiskDriveLetter P
-PersonalVDiskDriveSize 10 -ProvisioningSchemeName 'ExampleMachines' -RunAsynchronously -Scope @()
-UsePersonalVDiskStorage -VMCpuCount 1 -VMMemoryMB 1024
```

Creates a provisioning scheme object. This is a template for the machines that are to be created. It specifies the hypervisor, network, storage, memory, number of CPUs to be used etc. It takes parameters from the system already set up, such as the HostingUnit name and the path to the VM snapshot to be used for the machines to be created. This command makes a 'consolidated' copy of the VM snapshot being used and, as a result, the process can take time to complete.

In this example, the Studio script specified the -RunAsyncronous flag on this command. This means the command will return control to the administrator before it has completed, so you must wait for it to finish before performing any operations that require it to be complete. If this flag is not specified, the command runs synchronously in-line and control is not returned until the command completes (successfully or otherwise). You can check the status of an asynchronous task using the Get-ProvTask cmdlet. Supply the task ID returned from the operation that started the task; in this case, the New-ProvScheme cmdlet.

```
7. Set-BrokerCatalog  -AdminAddress 'ddc.dumdev.internal.citrix.com:80'
-LoggingId f39a2792-064a-43eb-97c7-397cc1238e46 -Name 'ExampleMachines'
-ProvisioningSchemeId 76125e3a-9001-4993-86b6-eefc85c87880
```

Updates the BrokerCatalog with the unique Id of the provisioning scheme created above.

```
8. Add-ProvSchemeControllerAddress  -AdminAddress 'ddc.dumdev.internal.citrix.com:80'
-ControllerAddress @('DDC.dumdev.internal.citrix.com') -LoggingId f39a2792-064a-43eb-97c7-397cc1238e46
-ProvisioningSchemeName 'ExampleMachines'
```

Adds a set of controller addresses to the provisioning scheme object. This is a list of addresses that the machines created can use to register with a Controller (broker) when deployed. The machines' registration addresses can be supplied in many ways; however, this information is required if the administrator wants to use the 'Allow Machine Creation Service to supply this' in the VDA installer. Changes to this list affect only machines created after the change, not existing machines.

9. Get-AcctADAccount -AdminAddress 'ddc.dumdev.internal.citrix.com:80'
-IdentityPoolUid b99aee6d-8772-4dbc-978b-8eb9a26e2407 -Lock $False -MaxRecordCount 2147483647
-State 'Available'
Studio gets a list of available Machine Identities from the Identity Pool so that, if existing accounts have been created in the past but are unused, these can be consumed instead of creating new accounts. Note that this is not required in a script because new accounts can be created instead, provided the script is running in a context that has permissions to do this. However, if the script does not have permissions to create accounts, change the script to consume available accounts (a separate process will be required to provide a pool of accounts into the Identity Pool, before running the script).

10. New-AcctADAccount -AdminAddress 'ddc.dumdev.internal.citrix.com:80' -Count 2
-IdentityPoolUid b99aee6d-8772-4dbc-978b-8eb9a26e2407 -LoggingId f39a2792-064a-43eb-97c7-397cc1238e46
Creates the required AD computer accounts in Active Directory. The script creates one account but, if required, it can create more using the 'Count' parameter of the command. The accounts are created into the OU defined in the provisioning scheme created above.

11. New-ProvVM -ADAccountName @('DUMDEV\Example-0001$','DUMDEV\Example-0002$')
-AdminAddress 'ddc.dumdev.internal.citrix.com:80' -LoggingId f39a2792-064a-43eb-97c7-397cc1238e46
-ProvisioningSchemeName 'ExampleMachines' -RunAsynchronously
Creates virtual machines, based on the template definition in the provisioning scheme created above. This process may take time to complete.

12. Lock-ProvVM -AdminAddress 'ddc.dumdev.internal.citrix.com:80'
-LoggingId f39a2792-064a-43eb-97c7-397cc1238e46 -ProvisioningSchemeName 'ExampleMachines'
-Tag 'Brokered' -VMID @('0710bb77-d01f-d006-4d67-5472e5cd349f')
Locks the provisioned virtual machines and prevents accidental modification of the virtual machine. Consumers of the SDK can use this to indicate that the virtual machine is in use and why it is locked. The script locks the VM with a tag of 'Brokered' to indicate the virtual machine is created and added to a Broker catalog and must not be deleted without first being removed from the catalog. You can set the Tag name to whatever is required.

13. New-BrokerMachine -AdminAddress 'ddc.dumdev.internal.citrix.com:80' -CatalogUid 1
-HostedMachineId '0710bb77-d01f-d006-4d67-5472e5cd349f' -HypervisorConnectionUid 1
-LoggingId f39a2792-064a-43eb-97c7-397cc1238e46
-MachineName 'S-1-5-21-3918710733-2340574387-1999698698-109114'
Creates a Broker Machine object. These are objects stored in the catalog which join the provisioned machine with the catalog.

14. Start-BrokerMachinePvdImagePrepare -AdminAddress 'ddc.dumdev.internal.citrix.com:80'
-InputObject @(2) -LoggingId f39a2792-064a-43eb-97c7-397cc1238e46
Requests the Broker Service to initiate a preparation operation for Personal vDisk. This is required to allow the machine to initialize the storage for Personal vDisk.

15. Stop-LogHighLevelOperation -AdminAddress 'ddc.dumdev.internal.citrix.com:80'
-HighLevelOperationId f39a2792-064a-43eb-97c7-397cc1238e46 -IsSuccessful $true
Stops the logged operation begun in the first step and indicates it was successful.

Customize the script

The following section shows how to convert and adapt the Studio output into a script that is more consumable. In addition to using variables and removing commands that are not required, it shows how to add machine creation into a loop so that you can control the number of machines created. Line numbers have been added for readability.

```
1. [CmdletBinding()]
param
(
   [Parameter(Mandatory=$true)] [string] $hostingUnitPath,
   [Parameter(Mandatory=$true)] [string] $catalogName,
   [string] $catalogDescription,
   [Parameter(Mandatory=$true)] [int] $numVmsToCreate,
   [string] $adminAddress,
   [Parameter(Mandatory=$true)] [string] $namingScheme,
   [string] $OU,
   [Parameter(Mandatory=$true)] [string] $domain,
   [Parameter(Mandatory=$true)] [string] $masterImagePath
)
2. Set-HypAdminConnection -AdminAddress $adminAddress

3. $hostingUnit = get-item $hostingUnitPath
```



```
4. $hostConnection = $hostingUnit.hypervisorConnection
5. $brokerHypConnection = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hostConnection.HypervisorConnectionUid
6. # Start logged operation
7. $loggingOp = Start-LogHighLevelOperation  -AdminAddress $adminAddress -Source 'Scripted'
-Text "Create Machine Catalog `'$catalogName`'"
8. $loggingId = $loggingOp.Id
9. # Create the broker catalog and the AD Identity account pool
10. $catalog = New-BrokerCatalog -AllocationType 'Permanent' -Description $catalogDescription -IsRemotePC $False
-MinimumFunctionalLevel 'L7' -Name $catalogName -PersistUserChanges 'OnPvd' -ProvisioningType 'MCS' -Scope @()
-SessionSupport 'SingleSession' -LoggingId $loggingId -AdminAddress $adminAddress
11. $adPool = New-AcctIdentityPool -IdentityPoolName $catalogName -NamingScheme $namingScheme
-NamingSchemeType 'Numeric' -OU $OU -Domain $domain -AllowUnicode -LoggingId $loggingId
-AdminAddress $adminAddress
12. Set-BrokerCatalogMetadata -CatalogId $catalog.Uid -Name 'Citrix_DesktopStudio_IdentityPoolUid'
-Value $adPool.IdentityPoolUid -LoggingId $loggingId  -AdminAddress $adminAddress

13. ###################################################################
14. #create the ProvisioningScheme and wait for it to complete (reporting progress)
15. $provSchemeTaskID = New-ProvScheme -ProvisioningSchemeName $catalogName -HostingUnitUID $hostingUnit.HostingUnitUID
-IdentityPoolUID $adpool.IdentityPoolUid -CleanOnBoot -MasterImageVM $masterImagePath -UsePersonalVDiskStorage
-PersonalVDiskDriveLetter P -PersonalVDiskDriveSize 10 -RunAsynchronously -LoggingId $loggingId -AdminAddress $adminAddress
16. $ProvTask = get-provTask -TaskID $provSchemeTaskID -AdminAddress $adminAddress
17. $taskProgress = 0
18. write-host "Creating New ProvScheme"
19. while ($provTask.Active -eq $true)
20. {
21.  # catch an uninitialized task progress, this occurs until the product initialized the value
22.  try {$totalPercent = if ($provTask.TaskProgress){$provTask.TaskProgress} else {0}} catch {}
23.  Write-Progress -activity "Creating Provisioning Scheme:" -status "$totalPercent% Complete:" -percentcomplete $totalPercent
24.  sleep 30
25.  $ProvTask = get-provTask -TaskID $provSchemeTaskID -AdminAddress $adminAddress
26. }
27. write-host "New ProvScheme Creation Finished"
28. $provScheme = get-provScheme -ProvisioningSchemeUID $provTask.ProvisioningSchemeUid
29. $controllers = Get-BrokerController | select DNSName
30. Add-ProvSchemeControllerAddress -ProvisioningSchemeUID $provScheme.ProvisioningSchemeUID -ControllerAddress $controllers
-LoggingId $loggingId -AdminAddress $adminAddress

31. ###################################################################
32. # Set the provisioning scheme id for the broker catalog
33. Set-BrokerCatalog -InputObject $catalog -ProvisioningSchemeId $provTask.ProvisioningSchemeUid
-LoggingId $loggingId -AdminAddress $adminAddress

34. ###################################################################
35. # create the AD accounts required and then create the Virtual machines (reporting progress)
36. $accts = New-AcctADAccount -IdentityPoolUid $adPool.IdentityPoolUid -Count $numVMsToCreate
-LoggingId $loggingId -AdminAddress $adminAddress
37. $provVMTaskID = New-ProvVM -ProvisioningSchemeUID $provScheme.ProvisioningSchemeUID
-ADAccountName $accts.SuccessfulAccounts -RunAsynchronously -LoggingId $loggingId -AdminAddress $adminAddress
38. # wait for the VMS to finish Provisioning
39. $ProvTask = get-provTask -TaskID $provVMTaskID -AdminAddress $adminAddress
40. while ($provTask.Active -eq $true)
41. {
42.    # catch an uninitialized task progress, this occurs until the product initialized the value
43.    try {$totalPercent = if ($provTask.TaskProgress){$provTask.TaskProgress} else {0}} catch {}
44.    Write-Progress -activity "Creating Machines:" -status "$totalPercent% Complete:" -percentcomplete $totalPercent
45.    sleep 5
46.    $ProvTask = get-provTask -TaskID $provVMTaskID -AdminAddress $adminAddress
47. }
48. write-host "VM Creation Finished"
49. # Lock the VMs and add them to the broker Catalog
50. $provisionedVMs = get-ProvVM -ProvisioningSchemeUID $provScheme.ProvisioningSchemeUID -AdminAddress $adminAddress
51. $provisionedVMs | Lock-ProvVM -ProvisioningSchemeUID $provScheme.ProvisioningSchemeUID -Tag 'Brokered'
```

-LoggingId $loggingId -AdminAddress $adminAddress
52. $provisionedVMs | ForEach-Object {New-BrokerMachine -CatalogUid $catalog.UID -HostedMachineId $_.VMId
-HypervisorConnectionUid $brokerHypConnection.UID -MachineName $_.ADAccountSid -LoggingId $loggingId -AdminAddress $adminAddress}
53. Stop-LogHighLevelOperation -IsSuccessful $true -HighLevelOperationId $loggingId -AdminAddress $adminAddress

Example: Create and configure a host

Apr 27, 2015

The following example shows how to create and configure a host.

Before you begin, make sure you follow the steps detailed in Get started with the SDK, which tells you how to use Studio to perform the operation you want to script (in this case, to create a host) and collect the log of SDK operations that Studio made to perform the task. This output can then be customized to produce a script for automating host creation.

Note: To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script. Line numbers and line breaks have been added to the script for readability.

Understand the script

The following section explains what each part of the script produced by Studio is doing. This will help you with the customization of your own script. Line numbers have been added for readability.

1. Get-LogSite -AdminAddress 'mycontroller.example.com:80'
Queries the configuration logging service to retrieve information about the site configuration.

2. Start-LogHighLevelOperation -AdminAddress 'mycontroller.example.com:80' -Source 'Studio'
-StartTime 14/08/2013 14:30:28 -Text 'Create Connection `''Example XenServer`'''
Starts a high-level logging operation with the configuration logging operation within which the rest of the commands will exist. Returns a log ID which is supplied to subsequent operations.

3. Set-HypAdminConnection -AdminAddress 'mycontroller.example.com:80'
Sets the location of the Host Service that will be used by the configuration cmdlets. Because the Host Service exposes a PowerShell provider, not all of the cmdlets can take an address for the service so this cmdlet sets a default location.

4. New-Item -ConnectionType 'XenServer' -HypervisorAddress @('http://xenhost1.example.com')
-LoggingId e355ce51-8cbb-400a-ae81-1fdc567239cb -Path @('XDHyp:\Connections\Example XenServer')
-Scope @() -Password ******** -UserName 'root'
Creates a connection to a XenServer (xenhost1.example.com). This is a non-persistent connection and is available only to this PowerShell runspace.

5. Stop-LogHighLevelOperation -AdminAddress 'mycontroller.example.com:80' -EndTime 14/08/2013 14:30:29
-HighLevelOperationId 'e355ce51-8cbb-400a-ae81-1fdc567239cb' -IsSuccessful $True
Stops the logged operation begun previously and indicates it was successful.

6. Get-LogSite -AdminAddress 'mycontroller.example.com:80'
Queries the configuration logging service to retrieve information about the site configuration.

7. Start-LogHighLevelOperation -AdminAddress 'mycontroller.example.com:80' -Source 'Studio'
-StartTime 14/08/2013 14:30:30 -Text 'Update Connection `''Example XenServer`'''
Starts a new high-level logging operation.

8. Set-HypAdminConnection -AdminAddress 'mycontroller.example.com:80'
Sets the Host Service address details again (note that this repetition is removed in the optimized script below).

9. Set-Item -HypervisorAddress @('http://xenhost1.example.com','http://xenhost2.example.com')
-LoggingId 44e15629-6906-4840-a36c-984aaf67be6d -PassThru -Path @('XDHyp:\Connections\Example XenServer')
-Password ******** -UserName 'root'
Updates the connection created in step 4. Because there is more than one XenServer in the pool, it supplies all the addresses to enable High Availability.

10. Stop-LogHighLevelOperation -AdminAddress 'mycontroller.example.com:80' -EndTime 14/08/2013 14:30:31
-HighLevelOperationId '44e15629-6906-4840-a36c-984aaf67be6d' -IsSuccessful $True
Stops the logging operation begun in step 7.

11. Get-LogSite -AdminAddress 'mycontroller.example.com:80'
Queries the configuration logging service to retrieve information about the site configuration.

12. Start-LogHighLevelOperation -AdminAddress 'mycontroller.example.com:80' -Source 'Studio'
-StartTime 14/08/2013 14:31:03 -Text 'Create Resources `''Example Resources`'' and Persist Connection `''Example XenServer`'''
Starts a new logging operation.

13. Set-HypAdminConnection -AdminAddress 'mycontroller.example.com:80'

Sets the Host Service address details again.

14. Get-ChildItem -Path @('XDHyp:\Connections')
Gets the contents of the host connection to populate the wizard dialogs.

15. Set-HypAdminConnection -AdminAddress 'mycontroller.example.com:80'
Sets the Host Service address details again.

16. Remove-Item -LoggingId 76caa3f4-df93-4cb2-b78d-6a8824766314 -Path @('XDHyp:\Connections\Example XenServer')
Removes the temporary connection created in the wizard.

17. Set-HypAdminConnection -AdminAddress 'mycontroller.example.com:80'
Sets the Host Service address details again.

18. New-Item -ConnectionType 'XenServer' -HypervisorAddress @('http://xenhost1.example.com','http://xenhost2.example.com')
-LoggingId 76caa3f4-df93-4cb2-b78d-6a8824766314 -Path @('XDHyp:\Connections\Example XenServer') -Persist
-Scope @() -Password ******** -UserName 'root'
Recreates the connection as a persistent connection which is written to the database and available to other PowerShell runspaces.

19. New-BrokerHypervisorConnection -AdminAddress 'mycontroller.example.com:80'
-HypHypervisorConnectionUid a14096ba-5074-44ff-b596-371e345c0449 -LoggingId 76caa3f4-df93-4cb2-b78d-6a8824766314
Adds the host connection to the Broker Service.

20. Set-HypAdminConnection -AdminAddress 'mycontroller.example.com:80'
Sets the Host Service address details again.

21. New-Item -HypervisorConnectionName 'Example XenServer' -LoggingId 76caa3f4-df93-4cb2-b78d-6a8824766314
-NetworkPath @('XDHyp:\Connections\Example XenServer\Network 0.network') -Path @('XDHyp:\HostingUnits\Example Resources')
-PersonalvDiskStoragePath @('XDHyp:\Connections\Example XenServer\Pvd Storage.storage')
-RootPath 'XDHyp:\Connections\Example XenServer' -StoragePath @('XDHyp:\Connections\Example XenServer\Primary OS.storage')
Creates the HostingUnit (referred to as Resources in Studio) using the information gathered in step 14.

22. Set-HypAdminConnection -AdminAddress 'mycontroller.example.com:80'
Sets the Host Service address details again.

23. Get-Item -Path @('XDHyp:\Connections\Example XenServer')
Retrieves the newly created object.

Stop-LogHighLevelOperation -AdminAddress 'mycontroller.example.com:80' -EndTime 14/08/2013 14:31:07
-HighLevelOperationId '76caa3f4-df93-4cb2-b78d-6a8824766314' -IsSuccessful $True
Stops the logged operation begun previously and indicates if it was successful.

Customize the script

The following section shows how to convert and adapt the Studio output into a script that is more consumable. The following script has been simplified so that, instead of creating a temporary host connection in the process of acquiring information in the wizards as in the Studio script above, a persistent connection is created. Information is then queried from within this to create the HostingUnit (Resources). Note that the LoggingId and HypHyperConnectionUid details are different.

Line numbers have been added for readability; each numbered item is a single PowerShell command.

1. Start-LogHighLevelOperation -AdminAddress 'mycontroller.example.com:80' -Source 'Studio'
-Text 'Create Connection `''Example XenServer`'''

2. Set-HypAdminConnection -AdminAddress 'mycontroller.example.com:80'

3. New-Item -ConnectionType 'XenServer' -HypervisorAddress @('http://xenhost1.example.com','
http://xenhost2.example.com')-LoggingId 76caa3f4-df93-4cb2-b78d-6a8824766314 -Path @('XDHyp:\Connections\Example XenServer')
-Persist -Scope @() -Password ******** -UserName 'root'

4. Get-ChildItem -Path @('XDHyp:\Connections')

5. New-BrokerHypervisorConnection -AdminAddress 'mycontroller.example.com:80' -HypHypervisorConnectionUid
a14096ba-5074-44ff-b596-371e345c0449 -LoggingId 76caa3f4-df93-4cb2-b78d-6a8824766314

6. New-Item -HypervisorConnectionName 'Example XenServer' -LoggingId 76caa3f4-df93-4cb2-b78d-6a8824766314
-NetworkPath @('XDHyp:\Connections\Example XenServer\Network 0.network') -Path @('XDHyp:\HostingUnits\Example Resources')
-PersonalvDiskStoragePath @('XDHyp:\Connections\Example XenServer\Pvd Storage.storage')
-RootPath 'XDHyp:\Connections\Example XenServer'
-StoragePath @('XDHyp:\Connections\Example XenServer\PrimaryOS.storage')

7. Stop-LogHighLevelOperation -AdminAddress 'mycontroller.example.com:80'
-HighLevelOperationId '76caa3f4-df93-4cb2-b78d-6a8824766314' -IsSuccessful $True

Example: Create a PvD Desktop

Apr 27, 2015

This document provides an example of a script that creates a Delivery Group containing Personal vDisk (PvD) desktops.

Before you begin, make sure you follow the steps detailed in Get started with the SDK, which shows you how to use Studio to perform the operation you want to script and collect the log of SDK operations that Studio made to perform the task. This output can then be customized to produce a script for automating the task.

Note: To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

The following section explains what each part of the script produced by Studio is doing. This will help you with the customization of your own script. Line numbers and line breaks have been added to the script for readability.

```
1. Start-LogHighLevelOperation  -AdminAddress 'test-ddc.mydomain.com:80' -Source 'Studio'
-StartTime 31/07/2013 10:08:58 -Text 'Create Delivery Group `''Win7 PvD Desktops`''
```
Starts a logged operation and returns a log ID which is supplied to subsequent operations to associate them with the wider task.

```
2. New-BrokerDesktopGroup  -AdminAddress 'test-ddc.mydomain.com:80' -ColorDepth 'TwentyFourBit'
-DeliveryType 'DesktopsOnly' -DesktopKind 'Private' -InMaintenanceMode $False -IsRemotePC $False
-LoggingId 846f2d42-a994-4bce-ab58-be05c8d73b99 -MinimumFunctionalLevel 'L7' -Name 'Win7 PvD Desktops'
-OffPeakBufferSizePercent 10 -PeakBufferSizePercent 10 -PublishedName 'Win7 PvD Desktops' -Scope @()
-SecureIcaRequired $False -SessionSupport 'SingleSession' -ShutdownDesktopsAfterUse $False -TimeZone 'GMT Standard Time'
```
Creates a new Delivery Group with options collected by the Studio wizard.

```
3. Add-BrokerMachinesToDesktopGroup  -AdminAddress 'test-ddc.mydomain.com:80' -Catalog 'win7-pvd'
-Count 2 -DesktopGroup 'Win7 PvD Desktops' -LoggingId 846f2d42-a994-4bce-ab58-be05c8d73b99
```
Adds the number of machines requested from the nominated catalog to the new Delivery Group.

```
4. Set-Variable  -Name 'brokerUsers' -Value @('S-1-5-21-3291547628-200264090-930806513-1104','S-1-5-21-3291547628-200264090-930806513-1105')
Get-BrokerUser  -AdminAddress 'test-ddc.mydomain.com:80' -Filter {(SID -in $brokerUsers)} -MaxRecordCount 2147483647
Remove-Variable  -Name 'brokerUsers'
New-BrokerUser  -AdminAddress 'test-ddc.mydomain.com:80' -Name 'MYDOMAIN\user1'
New-BrokerUser  -AdminAddress 'test-ddc.mydomain.com:80' -Name 'MYDOMAIN\user2'
```
The above commands are not required, Studio is verifying users.

```
5. Test-BrokerAssignmentPolicyRuleNameAvailable  -AdminAddress 'test-ddc.mydomain.com:80' -Name @('Win7 PvD Desktops')
```
Studio checks that the policy assignment name is available to use.

```
6. New-BrokerAssignmentPolicyRule  -AdminAddress 'test-ddc.mydomain.com:80' -DesktopGroupUid 41
-Enabled $True -IncludedUserFilterEnabled $False -LoggingId 846f2d42-a994-4bce-ab58-be05c8d73b99
-MaxDesktops 1 -Name 'Win7 PvD Desktops'
```
Create the new policy assignment rule for the Delivery Group. No users are specified here so all control is through the access policy rule.

```
7. Set-Variable  -Name 'brokerUsers' -Value @('S-1-5-21-3291547628-200264090-930806513-1104','S-1-5-21-3291547628-200264090-930806513-1105')
Get-BrokerUser  -AdminAddress 'test-ddc.mydomain.com:80' -Filter {(SID -in $brokerUsers)} -MaxRecordCount 2147483647
Remove-Variable  -Name 'brokerUsers'
New-BrokerUser  -AdminAddress 'test-ddc.mydomain.com:80' -Name 'MYDOMAIN\user1'
New-BrokerUser  -AdminAddress 'test-ddc.mydomain.com:80' -Name 'MYDOMAIN\user2'
```
The above commands are not required, Studio is performing further checks.

```
8. Test-BrokerAccessPolicyRuleNameAvailable  -AdminAddress 'test-ddc.mydomain.com:80'
-Name @('Win7 PvD Desktops_Direct')
```
Studio tests that the access policy rule name is available to use.

```
9. New-BrokerAccessPolicyRule  -AdminAddress 'test-ddc.mydomain.com:80' -AllowedConnections 'NotViaAG'
-AllowedProtocols @('HDX','RDP') -AllowRestart $True -DesktopGroupUid 41 -Enabled $True -IncludedSmartAccessFilterEnabled $True
-IncludedUserFilterEnabled $True -IncludedUsers @('MYDOMAIN\user1','MYDOMAIN\user2')
-LoggingId 846f2d42-a994-4bce-ab58-be05c8d73b99 -Name 'Win7 PvD Desktops_Direct'
```
Creates the access policy rule for the new desktop for non-NetScaler Gateway connections.

```
10. Test-BrokerAccessPolicyRuleNameAvailable  -AdminAddress 'test-ddc.mydomain.com:80' -Name @('Win7 PvD Desktops_AG')
New-BrokerAccessPolicyRule  -AdminAddress 'test-ddc.mydomain.com:80' -AllowedConnections 'ViaAG' -AllowedProtocols @('HDX','RDP')
-AllowRestart $True -DesktopGroupUid 41 -Enabled $True -IncludedSmartAccessFilterEnabled $True -IncludedSmartAccessTags @()
-IncludedUserFilterEnabled $True -IncludedUsers @('MYDOMAIN\user1','MYDOMAIN\user2')
-LoggingId 846f2d42-a994-4bce-ab58-be05c8d73b99 -Name 'Win7 PvD Desktops_AG'
```
Studio repeats this process for NetScaler Gateway connections.

```
11. Test-BrokerPowerTimeSchemeNameAvailable  -AdminAddress 'test-ddc.mydomain.com:80' -Name @('Win7 PvD Desktops_Weekdays')
New-BrokerPowerTimeScheme  -AdminAddress 'test-ddc.mydomain.com:80' -DaysOfWeek 'Weekdays'
```

```
-DesktopGroupUid 41 -DisplayName 'Weekdays' -LoggingId 846f2d42-a994-4bce-ab58-be05c8d73b99 -Name 'Win7 PvD Desktops_Weekdays'
-PeakHours @($False,$False,$False,$False,$False,$False,$False,$True,$True,$True,$True,$True,$True,$True,$True,
$True,$True,$True,$True,$False,$False,$False,$False,$False) -PoolSize @(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
Test-BrokerPowerTimeSchemeNameAvailable  -AdminAddress 'test-ddc.mydomain.com:80' -Name @('Win7 PvD Desktops_Weekend')
New-BrokerPowerTimeScheme  -AdminAddress 'test-ddc.mydomain.com:80' -DaysOfWeek 'Weekend' -DesktopGroupUid 41
-DisplayName 'Weekend' -LoggingId 846f2d42-a994-4bce-ab58-be05c8d73b99 -Name 'Win7 PvD Desktops_Weekend'
-PeakHours @($False,$False,$False,$False,$False,$False,$False,$True,$True,$True,$True,$True,$True,$True,$True,
$True,$True,$True,$True,$False,$False,$False,$False,$False) -PoolSize @(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
```

Studio checks that the names for the (optional) weekday and weekend power schemes are available, and adds these.

```
12. Stop-LogHighLevelOperation  -AdminAddress 'test-ddc.mydomain.com:80' -EndTime 31/07/2013 10:09:05
-HighLevelOperationId '846f2d42-a994-4bce-ab58-be05c8d73b99' -IsSuccessful $True
```

Stops the logged operation begun in step 1 and indicates it was successful.

Customize the script

This section shows how to convert and adapt the Studio output into a script that is more consumable.

The script creates a Delivery Group containing PvD desktops. The catalog specified in the parameters must exist already and be populated appropriately (with an allocation type of static and a PvD disk). The script is designed to be run from a Powershell command line logged on as a Citrix administrator. No checks are made for permissions; the script will fail if the user does not have the appropriate permissions.

```
<#
Sample usage:
.\CreatePvDGroup.ps1 `
-GroupName "Win7 PvD Desktops" `
-SrcCatalog "win7-pvd" `
-NumDesktops 2 `
-Users @('mydomain\user1','mydomain\user2') `
#>
Param(
[Parameter(Mandatory=$true)] [string] $GroupName,
[Parameter(Mandatory=$true)] [string] $SrcCatalog,
[Parameter(Mandatory=$true)] [int] $NumDesktops,
[Parameter(Mandatory=$true)] [array] $Users
[string] $AdminAddress
)
```

The table explains the parameters used in the script.

Parameter	Description
GroupName	The name of the new PvD desktop group
SrcCatalog	The name of the catalog to be used to create the PvD desktop. Create the catalog by specifying an allocation type of static. Machines must also have PvD disks.
NumDesktops	The number of machines to add to the PvD desktop group. If insufficient machines are available, as many as possible are added.
Users	Which users can access the group. This is a list of users or groups; for example, @('mydomain\Domain Users') or @('mydomain\user1','mydomain\user2')

```
Set-HypAdminConnection -AdminAddress $adminAddress
```

Specify the hypervisor admin connection to use. Removes the need for the -AdminAddress for some of the commands.

```
$peakPoolSize = 2
$weekendPoolSizeByHour = new-object int[] 24
$weekdayPoolSizeByHour = new-object int[] 24
9..17 | %{ $weekdayPoolSizeByHour[$_] = $peakPoolSize }
$peakHours = (0..23 | %{ $_ -ge 9 -and $_ -le 17 })
```

This creates 24 element arrays with a 1 or a 0 in each entry. Use these to specify when peak hours are for the power schedules for the Delivery Groups. Elements 9 to 17 (hours starting 09:00 to 17:00) for weekdays are set to 1, others are left at 0. Two unassigned machines are powered up during peak times, if available.

```
$logId = Start-LogHighLevelOperation `
   -Text "Create PvD desktop group" `
   -Source "Create PvD Desktop Group Script"
```

Start a new logged operation. This returns a log ID which is passed into subsequent operations to associate them with the create group task.

```
$grp = New-BrokerDesktopGroup `
   -DesktopKind 'Private' `
   -DeliveryType 'DesktopsOnly' `
   -LoggingId $logId.Id `
```



```
    -Name $GroupName `
    -PublishedName $GroupName `
    -SessionSupport 'SingleSession' `
    -ShutdownDesktopsAfterUse $False
$count = Add-BrokerMachinesToDesktopGroup `
    -Catalog $SrcCatalog `
    -Count $NumDesktops `
    -DesktopGroup $GroupName `
    -LoggingId $logId.Id
"$count machines added to the PvD desktop group"
```

Create the new Delivery Group, delivering private desktops. The catalog used must have been populated with suitable machines (permanent with a PvD disk). PublishedName is the name seen by end users; the following uses the same name as the group name.

```
New-BrokerAssignmentPolicyRule `
    -DesktopGroupUid $grp.Uid `
    -IncludedUserFilterEnabled $False `
    -LoggingId $logId.Id `
    -MaxDesktops 1 `
    -Name ($GroupName + '_AssignRule') `
    | Out-Null
```

Assigned desktops need an assignment policy. Disable user filter so that access is controlled entirely by access policy rules.

```
New-BrokerAccessPolicyRule `
    -AllowedConnections 'NotViaAG' `
    -AllowedProtocols @('HDX','RDP') `
    -AllowRestart $True `
    -DesktopGroupUid $grp.Uid `
    -IncludedSmartAccessFilterEnabled $True `
    -IncludedUserFilterEnabled $True `
    -IncludedUsers $Users `
    -LoggingId $logId.Id `
    -Name ($GroupName + '_Direct') `
    | Out-Null
New-BrokerAccessPolicyRule `
    -AllowedConnections 'ViaAG' `
    -AllowedProtocols @('HDX','RDP') `
    -AllowRestart $True `
    -DesktopGroupUid $grp.Uid `
    -IncludedSmartAccessFilterEnabled $True `
    -IncludedSmartAccessTags @() `
    -IncludedUserFilterEnabled $True `
    -IncludedUsers $Users `
    -LoggingId $logId.Id `
    -Name ($GroupName + '_AG') `
    | Out-Null
```

Specify any access restrictions: allow direct access using NetScaler Gateway, using HDX & RDP protocols. The user can request the desktop be restarted, if necessary.

```
New-BrokerPowerTimeScheme `
    -DaysOfWeek 'Weekdays' `
    -DesktopGroupUid $grp.Uid `
    -DisplayName 'Weekdays' `
    -LoggingId $logId.Id `
    -Name ($GroupName + '_Weekdays') `
    -PeakHours $peakHours `
    -PoolSize $weekdayPoolSizeByHour `
    | Out-Null
New-BrokerPowerTimeScheme `
    -DaysOfWeek 'Weekend' `
    -DesktopGroupUid $grp.Uid `
    -DisplayName 'Weekend' `
    -LoggingId $logId.Id `
    -Name ($GroupName + '_Weekend') `
    -PeakHours $peakHours `
    -PoolSize $weekendPoolSizeByHour `
    | Out-Null
```

Optional: Specify power schedules.

```
Stop-LogHighLevelOperation  -HighLevelOperationId $logId.Id -IsSuccessful $True
```

Stop configuration logging and indicate if successful or not.

Example: Get load balancing information

Apr 27, 2015

You can use Server OS Machines to deliver cost-effective applications and desktops hosted on server operating systems to multiple users.

To load balance Server OS Machines in a deployment, you use Citrix policies. There are several load balancing policy settings for enabling and configuring load management between servers delivering Windows Server OS machines. For more information, see the load management policy settings reference documentation. You work with policies through Studio or the Group Policy Management Console in Windows; see the Policies documentation for details.

To see the load, you can use either the Citrix Director or Studio consoles, or the PowerShell SDK. The following example shows how to use the PowerShell SDK to display the load.

Note: If you've used previous versions of XenDesktop, you may be familiar with the **qfarm /load** command. This tool is no longer available, but you can use PowerShell to display similar output as shown in the example below.

Example: Get load index values

To display a list of machines with their calculated/measured load index values, together with counts of sessions running on them:

1. Start a shell in PowerShell. For more information, see: XenApp and XenDesktop SDK.
2. Type:
   ```
   Get-BrokerMachine -SessionSupport MultiSession -Property 'DnsName','LoadIndex','SessionCount'
   ```
   Note: Load index values go up to 10000. They indicate VDA machine load calculated from the configured sources, such as number of sessions. A value of 10000 indicates a fully loaded VDA machine; the broker will not send another user session to that machine.

For more information and examples, see the cmdlet help for the get-brokermachine cmdlet and About topics such as about_broker_filtering-xd7.html. See: PowerShell cmdlet help.

PowerShell cmdlet help

Sep 16, 2014

This section provides the PowerShell help text for all cmdlets.

- Citrix.AdIdentity.Admin.V2
- Citrix.AppV.Admin.V1
- Citrix.Broker.Admin.V2
- Citrix.Configuration.Admin.V2
- Citrix.ConfigurationLogging.Admin.V1
- Citrix.DelegatedAdmin.Admin.V1
- Citrix.EnvTest.Admin.V1
- Citrix.Host.Admin.V2
- Citrix.MachineCreation.Admin.V2
- Citrix.Monitor.Admin.V1
- Citrix.Storefront.Admin.V1

Citrix.AdIdentity.Admin.V2

Sep 10, 2014

Overview

Name	Description
AcctAdIdentitySnapin	The Active Directory Identity Service PowerShell snap-in provides
Acct Filtering	Describes the common filtering options for XenDesktop cmdlets.

Cmdlets

Name	Description
Add-AcctADAccount	Import Active Directory computer accounts from Active Directory for use in the AD Identity Service.
Add-AcctIdentityPoolScope	Add the specified IdentityPool(s) to the given scope(s).
Copy-AcctIdentityPool	Copies an Identity Pool and its associated Identities to a new IdentityPool
Get-AcctADAccount	Gets the AD accounts stored in the AD Identity Service.
Get-AcctDBConnection	Gets the database string for the specified data store used by the AdIdentity Service.
Get-AcctDBSchema	Gets a script that creates the AdIdentity Service database schema for the specified data store.
Get-AcctDBVersionChangeScript	Gets a script that updates the AdIdentity Service database schema.
Get-AcctIdentityPool	Gets existing identity pools.
Get-AcctInstalledDBVersion	Gets a list of all available database schema versions for the AdIdentity Service.
Get-AcctScopedObject	Gets the details of the scoped objects for the AdIdentity Service.
Get-AcctService	Gets the service record entries for the AdIdentity Service.
Get-AcctServiceAddedCapability	Gets any added capabilities for the AdIdentity Service on the controller.

Name	Description
Get-AcctServiceInstance	Gets the service instance entries for the AdIdentity Service.
Get-AcctServiceStatus	Gets the current status of the AdIdentity Service on the controller.
New-AcctADAccount	Creates AD computer accounts in the specified identity pool.
New-AcctIdentityPool	Creates a new identity pool.
Remove-AcctADAccount	Removes AD computer accounts from an identity pool.
Remove-AcctIdentityPool	Removes identity pools.
Remove-AcctIdentityPoolMetadata	Removes metadata from the given IdentityPool.
Remove-AcctIdentityPoolScope	Remove the specified IdentityPool(s) from the given scope(s).
Remove-AcctServiceMetadata	Removes metadata from the given Service.
Rename-AcctIdentityPool	Renames an identity pool.
Repair-AcctADAccount	Resets the Active Directory machine password for the given accounts.
Reset-AcctServiceGroupMembership	Reloads the access permissions and configuration service locations for the AdIdentity Service.
Set-AcctDBConnection	Configures a database connection for the AdIdentity Service.
Set-AcctIdentityPool	Update parameters of an identity pool.
Set-AcctIdentityPoolMetadata	Adds or updates metadata on the given IdentityPool.
Set-AcctServiceMetadata	Adds or updates metadata on the given Service.
Test-AcctDBConnection	Tests a database connection for the AdIdentity Service.
Test-AcctIdentityPoolNameAvailable	Checks to ensure that the proposed name for an identity pool is unused.
Unlock-AcctADAccount	Unlocks AD accounts within the AD Identity Service.

Name	Description
Unlock-AcctIdentityPool	Unlocks identity pools.
Update-AcctADAccount	Refreshes the AD computer account state stored in the AD Identity Service.

about_AcctAdIdentitySnapin

Sep 10, 2014

TOPIC

about_AcctADIdentityServiceSnapin

SHORT DESCRIPTION

The Active Directory Identity Service PowerShell snap-in provides administrative functions for the Active Directory Identity Service.

COMMAND PREFIX

All commands in this snap-in have 'Acct' in their name.

LONG DESCRIPTION

The Active Directory Identity Service PowerShell snap-in enables both local and remote administration of the Active Directory Identity Service. It provides facilities to store details about Active Directory computer accounts that the Machine Creation Service can use.

The snap-in provides two main entities:

Identity

A representation of an Active Directory computer account that reflects the state of the account within the context of the Machine Creation Service. When an account is created by or imported into the Active Directory Identity Service, the account password is stored. Once the account is consumed by the Machine Creation Service, the password is discarded. For accounts registered with the Active Directory Identity Service, identities hold the following additional state information.

Available
The Active Directory account is registered with the service, the password for the account is known, and the account is available to be consumed by another service. Accounts that are successfully created with the New-AcctADAccount command or imported using the Add-ADAccount command, are initially assigned this state.

InUse
The Active Directory account is registered and has been consumed by another service. The password for the account is no longer known to the service.

Error
The Active Directory account is registered, but is missing,

disabled, or locked within Active Directory. Accounts that are not successfully created with the New-AcctADAccount command or imported using the Add-ADAccount command appear in this state. Use the Update-AcctADAccount and Repair-AcctADAccount commands to resolve issues with accounts in this state.

Tainted
The Active Directory account is registered and has been released by all the consuming services, but cannot be made available for use as the password is no longer known. Use the Repair-AcctADAccount command to reset account passwords and restore the account state to 'Available'.

Identities can also be marked as 'Locked' by the Machine Creation Service to indicate that they are in use and must not be changed. These services are also responsible for unlocking the Active Directory accounts when they no longer require exclusive access. Use the Unlock-AcctADAccount command to allow the lock to be overriden, if necessary.

Identity Pool

Containers for identities that can be configured with all the information required for new Active Directory accounts to be created. Alternatively, identity pools can be populated by importing accounts that already exist in Active Directory. All accounts registered with the Active Directory Identity Service must be placed into one of these containers. An identity can belong to more than one identity pool, but the state of the identity cannot be different in each pool. For example, an identity that is in use will be marked 'InUse' in all the identity pools of which it is part.

To avoid conflicting changes, identity pools can also be marked as 'Locked' during operations that modify the content of a pool. These operations are also responsible for unlocking the identity pool. Use the unlock-AcctIdentityPool command to allow the lock to be overridden, if necessary.

ACTIVE DIRECTORY PERMISSIONS

Account Creation (using the New-AcctADAccount command)

To use PowerShell to create new Active Directory accounts, the runspace

must be run using an account with sufficient permissions in the required Active Directory container (specified by the identity pool organizational unit parameter) for accounts to be created.

Import Accounts (using the Add-AcctADAccount command)

There are two modes for this operation: situations where the Active Directory account passwords are known and situations where the passwords are not known.

If the account passwords are known, the accounts can be imported without the need for administrative permissions in Active Directory. The accounts are imported and the password provided is used to change the existing password.

If the passwords are not known, the runspace must be run using an account that has permissions to reset the password for the accounts.

about_Acct_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```

retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

```
A120901
B220000
...
```

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

Add-AcctADAccount

Sep 10, 2014

Import Active Directory computer accounts from Active Directory for use in the AD Identity Service.

Syntax

```
Add-AcctADAccount [-IdentityPoolName] <String> -ADAccountName <String[]> [-Password <String>] [-SecurePassword <SecureString>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Add-AcctADAccount -IdentityPoolUid <Guid> -ADAccountName <String[]> [-Password <String>] [-SecurePassword <SecureString>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability for Active Directory computer accounts that already exist in Active Directory to be used by the Citrix AD Identity Service and the other Citrix Machine Creation Services.

All aspects of this command that need to make modifications to the accounts in Active Directory will do so using the account that the PowerShell runspace is using. This means that if the passwords need resetting for the accounts, the user performing the operation in PowerShell must have sufficient privileges in Active Directory for this operation to complete successfully.

The following rules apply to the importing of Active Directory accounts; If the current account password is supplied, the cmdlet will attempt to change the password so that it is known only to the Citrix Identity Service. This uses password change operations and does not need AD account administration permissions. If the current password is not supplied, the cmdlet will attempt to reset the password for the Active Directory account so that it is known only to the Citrix Identity Service. This requires the cmdlet to have enough privileges in Active Directory for the accounts' password reset to be available. Imported accounts in a disabled or locked state in Active Directory are imported with the account marked in an error state. If the identity pool into which the account is being imported does not have a domain set, it assumes the domain of the first account imported into it.

Related topics

New-AcctADAccount

Remove-AcctADAccount

Repair-AcctADAccount

Get-AcctADAccount

Update-AcctADAccount

Unlock-AcctADAccount

Parameters

-IdentityPoolName<String>

The identity pool name into which to add the imported accounts.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ADAccountName<String[]>

The Active Directory account name to be imported.

Active Directory accounts are accepted in the following formats: Fully qualified DN e.g. CN=MyComputer,OU=Computers,DC=MyDomain,DC=Com; UPN format e.g MyComputer@MyDomain.Com; Domain qualified e.g MyDomain\MyComputer.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IdentityPoolUid<Guid>

The unique identifier for the identity pool to which imported accounts are to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Password<String>

The current password for the computer account.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecurePassword<SecureString>

The current password for the account (provided in a Secure String class).

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.AccountOperationDetailedSummary

The Add-AcctADAccount returns an object that contains the following parameters;

SuccessfulAccountsCount <int>

The number of accounts that were added successfully

FailedAccountsCount <int>

The number of accounts that were not added.

FailedAccounts <Citrix.XDPowerShell.AccountError[]>

The list of accounts that failed to be added. Each one has the following properties;

ADAccountName <string>

ADAccountSid <String>

ErrorReason <AdIdentityStatus>

This can be one of the following

UnableToConvertDomain

UnableToAccessAccountProperties

IdentityNotLocatedInDomain

UnableToAccessAccountProperties

IdentityDuplicateObjectExists

IdentityObjectLocked

IdentityObjectInUse

FailedToConnectToDomainController

FailedToExecuteSearchInAD

FailedToAccessComputerAccountInAD

FailedToSetPasswordInAD

FailedToChangePasswordInAD

ADServiceDatabaseError

ADServiceDatabaseNotConfigured

ADServiceStatusInvalidDb

DiagnosticInformtion <Exception>

Any other error information

SuccessfulAccounts <Citrix.AdIdentity.Sdk.Identity[]>

The list of accounts that were successfully added. Each one has the following properties;

ADAccountSid <string>

The AD account SID for the imported account.

ADAccountName <string>

The AD account name for the imported account.

Domain <string>

The domain for the imported account.

State <Citrix.AdIdentity.Sdk.ADIdentityState>

The state for the account. This can be;

Available

The account is not used.

InUse

The account is in use.

Error

The account is in error (i.e. the account is locked or disabled in AD).

Tainted

The account is no longer used, but the password is no longer known.

Lock <Boolean>

The account is locked (in the database not in AD).

Notes

To maintain maximum security when using the command programmatically, Citrix recommends you use the 'SecurePassword' property instead of the 'Password' property.

In the case of failure, the following errors can result.

Error Codes

IdentityPoolAlreadyLocked

The specified identity pool was locked by another operation.

IdentityPoolNotFound

The specified identity pool was not found.

IdentityDuplicateObjectExists

The specified AD account already exists for the identity pool.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Add-AcctADAccount -IdentityPoolName MyPool -ADAccountName "Domain\account","Domain\account2" -OutVariable result

 SuccessfulAccounts            SuccessfulAccountsCount     FailedAccountsCount   FailedAccounts
 ------------------            -----------------------     -------------------   --------------
 {domain\account, domain\account2} 2                     0                     {}

       $result[0].SuccessfulAccounts

       ADAccountSid  : S-1-5-21-1315084875-1285793635-2418178940-2644
       ADAccountName : domain\account
       Domain        : Domain.com
       State         : Available
       Lock          : False

       ADAccountSid  : S-1-5-21-1315084875-1285793635-2418178940-2645
       ADAccountName : domain\account2
       Domain        : Domain.com
       State         : Available
       Lock          : False
```

Import the two accounts (account and account2) from AD into the identity Pool called "MyPool"

Add-AcctIdentityPoolScope

Sep 10, 2014

Add the specified IdentityPool(s) to the given scope(s).

Syntax

```
Add-AcctIdentityPoolScope [-Scope] <String[]> -InputObject <IdentityPool[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-AcctIdentityPoolScope [-Scope] <String[]> -IdentityPoolUid <Guid[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-AcctIdentityPoolScope [-Scope] <String[]> -IdentityPoolName <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The AddAcctIdentityPoolScope cmdlet is used to associate one or more IdentityPool objects with given scope(s).

There are multiple parameter sets for this cmdlet, allowing you to identify the IdentityPool objects in different ways:

- IdentityPool objects can be piped in or specified by the InputObject parameter

- The IdentityPoolUid parameter specifies objects by IdentityPoolUid

- The IdentityPoolName parameter specifies objects by IdentityPoolName (supports wildcards)

To add a IdentityPool to a scope you need permission to change the scopes of the IdentityPool and permission to add objects to all of the scopes you have specified.

If the IdentityPool is already in a scope, that scope will be silently ignored.

Related topics

Remove-AcctIdentityPoolScope

Get-AcctScopedObject

Parameters

-Scope<String[]>

Specifies the scopes to add the objects to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-InputObject<IdentityPool[]>

Specifies the IdentityPool objects to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-IdentityPoolUid<Guid[]>

Specifies the IdentityPool objects to be added by IdentityPoolUid.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-IdentityPoolName<String[]>

Specifies the IdentityPool objects to be added by IdentityPoolName.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

None

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

ScopeNotFound

One of the specified scopes was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command with the specified objects or scopes.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

c:\PS>Add-AcctIdentityPoolScope Finance -IdentityPoolUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
Adds a single IdentityPool to the 'Finance' scope.

---------- EXAMPLE 2 ----------

c:\PS>Add-AcctIdentityPoolScope Finance,Marketing -IdentityPoolUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
Adds a single IdentityPool to the multiple scopes.

---------- EXAMPLE 3 ----------

c:\PS>Get-AcctIdentityPool | Add-AcctIdentityPoolScope Finance
Adds all visible IdentityPool objects to the 'Finance' scope.

---------- EXAMPLE 4 ----------

c:\PS>Add-AcctIdentityPoolScope Finance -IdentityPoolName A*
Adds IdentityPool objects with a name starting with an 'A' to the 'Finance' scope.

Copy-AcctIdentityPool

Sep 10, 2014

Copies an Identity Pool and its associated Identities to a new IdentityPool

Syntax

```
Copy-AcctIdentityPool [-IdentityPoolName] <String> [-NewIdentityPoolName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Copy-AcctIdentityPool -IdentityPoolUid <Guid> [-NewIdentityPoolName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to copy an IdentityPool.

The new IdentityPool will contain all the accounts that were in the original pool and will have the same domain and OU set. The naming scheme will be unset and the StartCount will be set to 1.

Related topics

New-AcctIdentityPool

Get-AcctIdentityPool

Remove-AcctIdentityPool

Parameters

-IdentityPoolName<String>

The name of the identity pool that is to be copied.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IdentityPoolUid<Guid>

The unique identifier for the identity pool that is to be copied.

Required?	true
Default Value	

Accept Pipeline Input?	false

-NewIdentityPoolName<String>

The name for the new IdentityPool.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.IdentityPool

This object provides details of the new identity pool and contains the following information:

IdentityPoolName <string>

The name of the identity pool.

IdentityPoolUid <Guid>

The unique identifier for the identity pool.

NamingScheme <string>

The naming scheme for the identity pool.

NamingSchemeType <Citrix.XDInterServiceTypes.ADIdentityNamingScheme>

The naming scheme type for the identity pool. This can be one of the following:

Numeric - naming scheme uses numeric indexes

Alphabetic - naming scheme uses alphabetic indexes

StartCount <int>

The next index to be used when creating an identity from the identity pool.

OU <string>

The Active Directory distinguished name for the OU in which accounts created from this identity pool will be created.

Domain <string>

The Active Directory domain that accounts in the pool belong to.

Lock <Boolean>

Indicates whether the identity pool is locked.

Notes

In the case of failure, the following errors can result.

Error Codes

IdentityPoolDuplicateObjectExists

An identity pool with the same name exists already.

IdentityPoolObjectNotFound

The identity pool to be modified could not be located.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Get-AcctADAccount

Sep 10, 2014

Gets the AD accounts stored in the AD Identity Service.

Syntax

Get-AcctADAccount [-IdentityPoolName <String>] [-ADAccountSid <String>] [-Domain <String>] [-State <ADIdentityState>] [-Lock <Boolean>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Get-AcctADAccount [-IdentityPoolUid <Guid>] [-ADAccountSid <String>] [-Domain <String>] [-State <ADIdentityState>] [-Lock <Boolean>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to locate the AD accounts stored within the AD Identity Service and view the state of the accounts.

Related topics

New-AcctADAccount

Add-AcctADAccount

Remove-AcctADAccount

Unlock-AcctADAccount

Update-AcctADAccount

Repair-AcctADAccount

Parameters

-ADAccountSid<String>

The AD Account SID of the account.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Domain<String>

The domain of the account (this is in dns format).

Required?	false

Default Value	
Accept Pipeline Input?	false

-State<ADIdentityState>

The current state of the identity stored in the AD Identity Service for the AD account.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Lock<Boolean>

Indicates if the account is locked in the AD Identity Service.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

See about_Acct_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

See about_Acct_Filtering for details.

Required?	false

Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

See about_Acct_Filtering for details.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

See about_Acct_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Filter<String>

See about_Acct_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

-IdentityPoolName<String>

The name of the identity pool to which the account is registered.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IdentityPoolUid<Guid>

The unique identifier for the identity pool that the account is registered to.

Required?	false
Default Value	
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.IdentityInPool

The Get-AcctADAccount returns an object that contains the following parameters

ADAccountSid <string>

The AD account SID for the retrieved account.

ADAccountName <string>

The AD account name for the retrieved account.

Domain <string>

The domain for the imported account.

State <Citrix.XDInterServiceTypes.ADIdentityState>

The state for the account. This can be;

Available

The account is not used.

InUse

The account is in use.

Error

The account is in error (i.e. the account is locked or disabled in AD).

Tainted

The account is no longer used, but the password is no longer known.

Lock <Boolean>

The account is locked (in the database not in AD).

IdentityPoolName <System.String>

The name of the containing identity pool.

IdentityPoolUid <System.Guid>

The GUID identifying the containing identity pool.

Notes

In the case of failure the following errors can result.

Error Codes

PartialData

Only a subset of the available data was returned.

CouldNotQueryDatabase

The query required to get the database was not defined.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

CommunicationError

An error occurred while communicating with the service.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\>Get-AcctADAccount
```

Return all the AD accounts that are registered in the AD Identity Service.

---------- EXAMPLE 2 ----------

```
C:\>Get-AcctADAccount -IdentityPoolName MyPool -Lock $false
```

Return all the AD accounts that are registered in the AD Identity Service in the identity pool called "MyPool" that are also locked.

---------- EXAMPLE 3 ----------

```
C:\>Get-AcctADAccount -Filter {IdentityPoolName -Like "p*" -or IdentityPoolName -eq "MyPool"}
```

Return all the AD accounts that are registered in the AD Identity Service in the identity pool called "MyPool" or in an identity pool that has a name that starts with a 'p'. For full details of the advanced filtering aspects of this command see about_Acct_Filtering.

Get-AcctDBConnection

Sep 10, 2014

Gets the database string for the specified data store used by the AdIdentity Service.

Syntax

```
Get-AcctDBConnection [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the database connection string for the specified data store.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

Related topics

Get-AcctServiceStatus

Set-AcctDBConnection

Test-AcctDBConnection

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

system.string

The database connection string configured for the AdIdentity Service.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the AdIdentity Service has not been specified.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AcctDBConnection

Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True
```

Get the database connection string for the AdIdentity Service.

Get-AcctDBSchema

Sep 10, 2014

Gets a script that creates the AdIdentity Service database schema for the specified data store.

Syntax

Get-AcctDBSchema [-DatabaseName <String>] [-ServiceGroupName <String>] [-ScriptType <ScriptTypes>] [-LocalDatabase] [-Sid <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets SQL scripts that can be used to create a new AdIdentity Service database schema, add a new AdIdentity Service to an existing site, remove a AdIdentity Service from a site, or create a database server logon for a AdIdentity Service. If no Sid parameter is provided, the scripts obtained relate to the currently selected AdIdentity Service instance, otherwise the scripts relate to AdIdentity Service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied. The current service instance is that on the local machine, or that explicitly specified by the last usage of the -AdminAddress parameter to a AdIdentity SDK cmdlet. The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured. The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SMDCMD mode'. The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to AdIdentity Service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to AdIdentity Service roles

If ScriptType is Evict, the returned script contains:

o Removal of AdIdentity Service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database. You do not need to configure a database before using this command.

Related topics

Set-AcctDBConnection

Parameters

-DatabaseName<String>

Specifies the name of the database for which the schema will be generated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the AdIdentity services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<ScriptTypes>

Specifies the type of database script returned. Available script types are:

Database

Returns a full database script that can be used to create a database schema for the AdIdentity Service in a database instance that does not already contain a schema for this service. The DatabaseName and ServiceGroupName parameters must be specified to create a script of this type.

Instance

Returns a permissions script that can be used to add further AdIdentity services to an existing database instance that already contains the full AdIdentity service schema, associating the services to the Service Group. The Sid parameter can optionally be specified to create a script of this type.

Login

Returns a database logon script that can be used to add the required logon accounts to an existing database instance that contains the AdIdentity Service schema. This is used primarily when creating a mirrored database environment. The

DatabaseName parameter must be specified to create a script of this type.

Evict

Returns a script that can be used to remove the specified AdIdentity Service from the database entirely. The DatabaseName and Sid parameters must be specified to create a script of this type.

Required?	false
Default Value	Database
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for AdIdentity services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Sid<String>

Specifies the SID of the controller on which the AdIdentity Service instance to remove from the database is running.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.string

A string containing the required SQL script for application to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AcctDBSchema -DatabaseName MyDB -ServiceGroupName  MyServiceGroup > c:\AcctSchema.sql
```

Get the full database schema for site data store of the AdIdentity Service and copy it to a file called 'c:\AcctSchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a AdIdentity Service site schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-AcctDBSchema -DatabaseName MyDB -scriptType Login > c:\AdIdentityLogins.sql
```

Get the logon scripts for the AdIdentity Service.

Get-AcctDBVersionChangeScript

Sep 10, 2014

Gets a script that updates the AdIdentity Service database schema.

Syntax

```
Get-AcctDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a database script that can be used to upgrade or downgrade the site or secondary schema for the AdIdentity Service from the current schema version to a different version.

Related topics

Get-AcctInstalledDBVersion

Parameters

-DatabaseName<String>

Specifies the name of the database instance to which the update applies.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

Specifies the version of the database you want to update to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

A PSObject containing the required SQL script for application to a database.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any AdIdentity services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-AcctServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the AdIdentity Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $update = Get-AcctDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-AcctIdentityPool

Sep 10, 2014

Gets existing identity pools.

Syntax

Get-AcctIdentityPool [[-IdentityPoolName] <String>] [-IdentityPoolUid <Guid>] [-Lock <Boolean>] [-ScopeId <Guid>] [-ScopeName <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to locate existing identity pools.

Related topics

New-AcctIdentityPool

Remove-AcctIdentityPool

Rename-AcctIdentityPool

Set-AcctIdentityPool

Parameters

-IdentityPoolName<String>

The name of the identity pool.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IdentityPoolUid<Guid>

The unique identifier for the identity pool.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Lock<Boolean>

Whether the identity pool is locked or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScopeId<Guid>

Gets only results with a scope matching the specified scope identifier.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScopeName<String>

Gets only results with a scope matching the specified scope name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

See about_Acct_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

See about_Acct_Filtering for details.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

See about_Acct_Filtering for details.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

See about_Acct_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Filter<String>

See about_Acct_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host

name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.IdentityPool

This object provides details of the identity pool and contains the following information:

IdentityPoolName <string>

The name of the identity pool.

IdentityPoolUid <Guid>

The unique identifier for the identity pool.

NamingScheme <string>

The naming scheme for the identity pool.

NamingSchemeType <Citrix.XDInterServiceTypes.ADIdentityNamingScheme>

The naming scheme type for the identity pool. This can be one of the following:

Numeric - naming scheme uses numeric indexes

Alphabetic - naming scheme uses alphabetic indexes

StartCount <int>

The next index to be used when creating an identity from the identity pool.

OU <string>

The Active Directory distinguished name for the OU in which accounts created from this identity pool will be created.

Domain <string>

The Active Directory domain that accounts in the pool belong to.

Lock <Boolean>

Indicates if the identity pool is locked.

Notes

In the case of failure, the following errors can result.

Error Codes

PartialData

Only a subset of the available data was returned.

CouldNotQueryDatabase

The query required to get the database was not defined.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

CommunicationError

An error occurred while communicating with the service.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS>Get-AcctIdentityPool

IdentityPoolName : MyPool
IdentityPoolUid  : 22072d9e-6a8f-494b-a5bc-2ef18ca4b915
NamingScheme     : Acc####
NamingSchemeType : Numeric
StartCount       : 1
OU               :
Domain           : mydomain.com
Lock             : True

IdentityPoolName : MyPool2
IdentityPoolUid  : 03743136-e43b-4a87-af74-ab71686b3c16
```



```
NamingScheme    : Test####
NamingSchemeType : Alphabetic
StartCount      : 1
OU              :
Domain          : mydomain.com
Lock            : False
```

Gets all the identity pools.

---------- EXAMPLE 2 ----------

```
C:\PS>Get-AcctIdentityPool -IdentityPoolName M*

IdentityPoolName : MyPool
IdentityPoolUid  : 22072d9e-6a8f-494b-a5bc-2ef18ca4b915
NamingScheme     : Acc####
NamingSchemeType : Numeric
StartCount       : 1
OU               :
Domain           : mydomain.com
Lock             : True
```

Gets all the identity pools beginning with the character 'M'.

Get-AcctInstalledDBVersion

Sep 10, 2014

Gets a list of all available database schema versions for the AdIdentity Service.

Syntax

```
Get-AcctInstalledDBVersion [-Upgrade] [-Downgrade] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the current version of the AdIdentity Service database schema, if no flags are set, otherwise returns versions for which upgrade or downgrade scripts are available and have been stored in the database.

Related topics

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Version

The Get-AcctInstalledDbVersion command returns objects containing the new definition of the AdIdentity Service database schema version.

Major <Integer>

Minor <Integer>

Build <Integer>

Revision <Integer>

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the AdIdentity Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AcctInstalledDBVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      6      0      0
```

Get the currently installed version of the AdIdentity Service database schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-AcctInstalledDBVersion -Upgrade

Major  Minor  Build  Revision
-----  -----  -----  --------
6      0      0      0
```

Get the versions of the AdIdentity Service database schema for which upgrade scripts are supplied.

Get-AcctScopedObject

Sep 10, 2014

Gets the details of the scoped objects for the AdIdentity Service.

Syntax

Get-AcctScopedObject [-ScopeId <Guid>] [-ScopeName <String>] [-ObjectType <ScopedObjectType>] [-ObjectId <String>] [-ObjectName <String>] [-Description <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns a list of directly scoped objects including the names and identifiers of both the scope and object as well as the object description for display purposes.

There will be at least one result for every directly scoped object. When an object is associated with multiple scopes the output contains one result per scope duplicating the object details.

No records are returned for the All scope, though if an object is not in any scope a result with a null ScopeId and ScopeName will be returned.

Related topics

Parameters

-ScopeId<Guid>

Gets scoped object entries for the given scope identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ScopeName<String>

Gets scoped object entries with the given scope name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ObjectType<ScopedObjectType>

Gets scoped object entries for objects of the given type.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ObjectId<String>

Gets scoped object entries for objects with the specified object identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ObjectName<String>

Gets scoped object entries for objects with the specified object identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Gets scoped object entries for objects with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Acct_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Acct_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.ScopedObject

The Get-AcctScopedObject command returns an object containing the following properties:

ScopeId <Guid?>

Specifies the unique identifier of the scope.

ScopeName <String>

Specifies the display name of the scope.

ObjectType <ScopedObjectType>

Type of the object this entry relates to.

ObjectId <String>

Unique identifier of the object.

ObjectName <String>

Display name of the object

Description <String>

Description of the object (possibly $null if the object type does not have a description).

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AcctScopedObject -ObjectType Scheme

ScopeId    : eff6f464-f1ee-4442-add3-99982e0cec01
ScopeName  : Sales
ObjectType : Scheme
ObjectId   : cd4174ee-9e4b-4e57-b126-9dbf757fe493
ObjectName : MyExampleScheme
Description : Test scheme

ScopeId    : 304e0fa7-d390-47f0-a94f-7e956a324c41
ScopeName  : Finance
ObjectType : Scheme
ObjectId   : cd4174ee-9e4b-4e57-b126-9dbf757fe493
ObjectName : MyExampleScheme
Description : Test scheme

ScopeId    :
ScopeName  :
ObjectType : Scheme
ObjectId   : 5062e46b-71bc-4ac9-901a-30fe6797e2f6
ObjectName : AnotherScheme
Description : Another scheme in no scopes
```

Gets all of the scoped objects with type Scheme. The example output shows a scheme object (MyExampleScheme) in two scopes Sales and Finance, and another scheme (AnotherScheme) that is not in any scope. The ScopeId and ScopeName values returned are null in the final record.

Get-AcctService

Sep 10, 2014

Gets the service record entries for the AdIdentity Service.

Syntax

Get-AcctService [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns instances of the AdIdentity Service that the service publishes. The service records contain account security identifier information that can be used to remove each service from the database.

A database connection for the service is required to use this command.

Related topics

Parameters

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Acct_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Acct_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.Service

The Get-AcctServiceInstance command returns an object containing the following properties.

Uid <Integer>

Specifies the unique identifier for the service in the group. The unique identifier is an index number.

ServiceHostId <Guid>

Specifies the unique identifier for the service instance.

DNSName <String>

Specifies the domain name of the host on which the service runs.

MachineName <String>

Specifies the short name of the host on which the service runs.

CurrentState <Citrix.Fma.Sdk.ServiceCore.ServiceState>

Specifies whether the service is running, started but inactive, stopped, or failed.

LastStartTime <DateTime>

Specifies the date and time at which the service was last restarted.

LastActivityTime <DateTime>

Specifies the date and time at which the service was last stopped or restarted.

OSType

Specifies the operating system installed on the host on which the service runs.

OSVersion

Specifies the version of the operating system installed on the host on which the service runs.

ServiceVersion

Specifies the version number of the service instance. The version number is a string that reflects the full build version of the service.

DatabaseUserName <string>

Specifies for the service instance the Active Directory account name with permissions to access the database. This will be either the machine account or, if the database is running on a controller, the NetworkService account.

Sid <string>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

ActiveSiteServices <string[]>

Specifies the names of active site services currently running in the service. Site services are components that perform long-running background processing in some services. This field is empty for services that do not contain site services.

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-AcctService

Uid             : 1
ServiceHostId     : aef6f464-f1ee-4042-a523-66982e0cecd0
DNSName           : MyServer.company.com
MachineName       : MYSERVER
CurrentState      : On
LastStartTime     : 04/04/2011 15:25:38
LastActivityTime  : 04/04/2011 15:33:39
OSType            : Win32NT
OSVersion         : 6.1.7600.0
ServiceVersion    : 5.1.0.0
DatabaseUserName  : NT AUTHORITY\NETWORK SERVICE
SID               : S-1-5-21-2316621082-1546847349-2782505528-1165
ActiveSiteServices : {MySiteService1, MySiteService2...}
```

Get all the instances of the AdIdentity Service running in the current service group.

Get-AcctServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the AdIdentity Service on the controller.

Syntax

```
Get-AcctServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the AdIdentity Service on the controller to be detected.

You do not need to configure a database connection before using this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AcctServiceAddedCapability
```

Get the added capabilities of the AdIdentity Service.

Get-AcctServiceInstance

Sep 10, 2014

Gets the service instance entries for the AdIdentity Service.

Syntax

```
Get-AcctServiceInstance [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns service interfaces published by the instance of the AdIdentity Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.ServiceInstance

The Get-AcctServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a

central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

Specifies the service instance type. For this service, the service instance type is always Acct.

Address

Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

SDK - for PowerShell operations

InterService - for operations between different services

Peer - for communications between services of the same type

Metadata <Citrix.AdIdentity.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AcctServiceInstance

Address          : http://MyServer.com:80/Citrix/AdIdentityService
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         :
MetadataMap      :
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName  : MyServiceGroup
ServiceGroupUid   : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType      : Acct
Version          : 1

Address          : http://MyServer.com:80/Citrix/AdIdentityService/IServiceApi
Binding          : wcf_HTTP_kerb
InterfaceType    : InterService
Metadata         :
MetadataMap      :
```



```
ServiceAccount     : ENG\MyAccount
ServiceAccountSid  : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName   : MyServiceGroup
ServiceGroupUid    : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType        : Acct
Version            : 1
```

Get all instances of the AdIdentity Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-AcctServiceStatus

Sep 10, 2014

Gets the current status of the AdIdentity Service on the controller.

Syntax

```
Get-AcctServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the AdIdentity Service on the controller to be monitored. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured.

Related topics

Set-AcctDBConnection

Test-AcctDBConnection

Get-AcctDBConnection

Get-AcctDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-AcctServiceStatus command returns an object containing the status of the AdIdentity Service together with extra diagnostics information.

DBUnconfigured

The AdIdentity Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the AdIdentity Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the AdIdentity Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the AdIdentity Service currently in use is incompatible with the version of the AdIdentity Service schema on the database. Upgrade the AdIdentity Service to a more recent version.

DBOlderVersionThanService

The version of the AdIdentity Service schema on the database is incompatible with the version of the AdIdentity Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The AdIdentity Service is running and is connected to a database containing a valid schema.

Failed

The AdIdentity Service has failed.

Unknown

(0) The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-AcctServiceStatus
```

DBUnconfigured
Get the current status of the AdIdentity Service.

New-AcctADAccount

Sep 10, 2014

Creates AD computer accounts in the specified identity pool.

Syntax

New-AcctADAccount [-IdentityPoolName] <String> -ADAccountName <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-AcctADAccount [-IdentityPoolName] <String> -Count <Int32> [-StartCount <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-AcctADAccount -IdentityPoolUid <Guid> -Count <Int32> [-StartCount <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-AcctADAccount -IdentityPoolUid <Guid> -ADAccountName <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to create new AD computer accounts and register them in an already existing identity pool.

The accounts are created using the information stored in the identity pool. This provides the account name (via the Naming Scheme property and Start Count), domain, and OU.

The runspace used for this command must have sufficient privileges in Active Directory to create the new computer accounts.

The AD account names will pad the index to use all the space specified in the identity pool naming scheme (e.g. "acc###" will become "acc001"). However, if the index overflows the available space the cmdlet expands the format to use the next incremental number (e.g. "acc###" will become "acc1000" if the index is 10000, which cannot fit into the three '#' placeholders). If this expanded name exceeds the 15 character name limit, the accounts are not created.

There can be only one creation process running for a specific identity pool at any one time. Attempting to start another account creation process while an existing one is executing results in an error being returned.

Related topics

Add-AcctADAccount

Remove-AcctADAccount

Get-AcctADAccount

Repair-AcctADAccount

Unlock-AcctADAccount

Update-AcctADAccount

Parameters

-IdentityPoolName<String>

The name of the identity pool in which to create the accounts.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ADAccountName<String[]>

The AD account names to be created. These are just the simple machine account names e.g. MyVM001

Required?	true
Default Value	
Accept Pipeline Input?	false

-Count<Int32>

The number of accounts to create.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IdentityPoolUid<Guid>

The unique identifier for the identity pool in which the accounts will be created.

Required?	true
Default Value	
Accept Pipeline Input?	false

-StartCount<Int32>

The start index for the create process.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.AccountOperationDetailedSummary

The Add-AcctADAccount returns an object that contains the following parameters;

SuccessfulAccountsCount <int>

The number of accounts that were added successfully

FailedAccountsCount <int>

The number of accounts that were not added.

FailedAccounts <Citrix.AdIdentity.Sdk.AccountError[]>

The list of accounts that failed to be added. Each one has the following parameters;

ADAccountName <string>

ADAccountSid <String>

ErrorReason <string>

This can be one of the following

IdentityDuplicateObjectExists

An identity with the same SID already exists.

ADServiceDatabaseError

An error occurred in the service while attempting a database operation.

ADServiceDatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ADServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for for various reasons.

FailedToConnectToDomainController

Contacting Active Directory failed.

FailedToGetOrganizationUnitInAD

Failed to access the OU in Active Directory.

FailedToGetDefaultComputerContainerInAD

Failed to access the default computers container in Active Directory.

FailedToCreateComputerAccountInAD

Failed to create the computer account in Active Directory.

FailedToAccessComputerAccountInAD

Failed to read the newly created computer account in Active Directory.

FailedToGetSidFromAD

Failed to get the SID for the created account from Active Directory.

FailedToSetSamAccountNameInAD

Failed to set the SAM account name in Active Directory for the account created.

FailedToSetUserAccountControlInAD

Failed to set the user account controller properties for the account created in Active Directory.

FailedToSaveChangeInAD

Failed to save the changes made to the created computer account in Active Directory.

FailedToSetPasswordInAD

Failed to set the password for the created computer account in Active Directory.

FailedToEnableAccountInAD

Failed to enable the newly created computer account in Active Directory.

ComputerNameAlreadyInUseInAD

The computer name for the computer to create is in use in Active Directory.

FailedToGetDistinguishedNameInAD

Failed to get the distinguished name for the created computer account in ActiveDirectory.

FailedToSetDnsHostNameInAD

Failed to set the Dns Host Name property for the created computer account in ActiveDirectory.

FailedToSetDisplayNameInAD

Failed to set the DisplayName property for the created computer account in ActiveDirectory.

FailedToWriteServicePrincipalNameInAD

Failed to set the ServicePrincipalName property for the created computer account in ActiveDirectory.

DiagnosticInformtion <Exception>

Any other error information

SuccessfulAccounts <Citrix.AdIdentity.Sdk.Identity[]>

The list of accounts that were successfully added. Each object

provides details of the identity and contains the following information:

ADAccountSID <string>

The Sid of the identity.

ADAccountName <string>

The account name for the identity.

Domain <string>

The domain name that the account was created in.

State <string>

The current state of the AD account. This can be one of the following:

Error

The account is locked or disabled in AD.

Available

The account is in AD and available to be consumed by the other Machine Creation Services.

InUse

The account is in AD and is being consumed by the other Machine Creation Services.

Tainted

The account is in AD and no longer consumed by other Machine Creation Services. However, the password is no longer known so cannot be reused without 'Repairing' the account. See repair-AcctADAccount for details.

Lock <Boolean>

Indicates if the identity pool is locked.

Notes

In the case of failure, the following errors can result.

Error Codes

NamingSchemeNotSpecifiedForIdentityPool

No naming scheme is defined in the specified identity pool.

IdentityPoolObjectNotFound

The specified identity pool was not located.

IdentityPoolAlreadyLocked

The specified identity pool is locked.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>New-AcctADAccount -IdentityPoolName MyPool -Count 2 -OutVariable result

        SuccessfulAccounts            SuccessfulAccountsCount      FailedAccountsCount    FailedAccounts
        ------------------            -----------------------      -------------------    --------------
        {MyDomain\ACC001, MyDomain\ACC002} 2                       0                {}

        $result[0].SuccessfulAccounts

        ADAccountSid  : S-1-5-21-1315084875-1285793635-2418178940-2684
        ADAccountName : MyDomain\ACC001
        Domain        : MyDomain.com
        State         : Available
        Lock          : False

        ADAccountSid  : S-1-5-21-1315084875-1285793635-2418178940-2685
        ADAccountName : MyDomain\ACC002
        Domain        : MyDomain.com
        State         : Available
        Lock          : False
```

Creates two new AD accounts and registers them in the identity pool called "MyPool".

---------- EXAMPLE 2 ----------

```
c:\PS>New-AcctADAccount -IdentityPoolName MyPool -Count 2 -StartCount 50 -OutVariable result

        SuccessfulAccounts            SuccessfulAccountsCount      FailedAccountsCount    FailedAccounts
```



```
------------------           ------------------------     --------------------   --------------
{MyDomain\ACC050, MyDomain\ACC051} 2                      0                 {}

$result[0].SuccessfulAccounts

ADAccountSid  : S-1-5-21-1315084875-1285793635-2418178940-2686
ADAccountName : MyDomain\ACC050
Domain        : MyDomain.com
State         : Available
Lock          : False

ADAccountSid  : S-1-5-21-1315084875-1285793635-2418178940-2687
ADAccountName : MyDomain\ACC051
Domain        : MyDomain.com
State         : Available
Lock          : False
```

Creates two new AD accounts and registers them in the identity pool called "MyPool", starting from an index of 50.

New-AcctIdentityPool

Sep 10, 2014

Creates a new identity pool.

Syntax

New-AcctIdentityPool -IdentityPoolName <String> [-NamingScheme <String>] [-NamingSchemeType <ADIdentityNamingScheme>] [-OU <String>] [-Domain <String>] [-AllowUnicode] [-StartCount <Int32>] [-Scope <String[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to create identity pools that can be used to store AD computer accounts.

The naming scheme, naming scheme type, and domain must be specified if the identity pool is to be used to create new accounts.

Each identity pool is tied to a single domain. All the identities in an identity pool belong to the same domain. If the domain is not specified by a parameter to this command the domain will be set when an account is imported into it.

Related topics

Remove-AcctIdentityPool

Rename-AcctIdentityPool

Set-AcctIdentityPool

Test-AcctIdentityPoolNameAvailable

New-AcctADAccount

Parameters

-IdentityPoolName<String>

The name of the identity pool. This must not contain any of the following characters \/:;#.*?=<>|[]()'"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-NamingScheme<String>

Defines the template name for AD accounts created in the identity pool. The scheme can consist of fixed characters and a variable part defined by '#' characters. There can be only one variable region defined. The number of '#' characters defines the minimum length of the variable region. For example, a naming scheme of H#### could create accounts called H0001, H0002 (for a numeric scheme type) or HAAAA, HAAAB (for an alphabetic type).

Citrix recommends that you define a naming scheme that will not clash with accounts which already exist in AD; account creation will fail if a clash occurs.

There are restrictions on what constitutes a valid computer name: Minimum name length: 2 (DNS) Maximum name length: 15 bytes (NetBIOS) The following characters are not allowed in a computer name: backslash (\) slash mark (/) colon (:) asterisk (*) question mark (?) quotation mark (") less than sign (<) greater than sign (>) vertical bar (|) comma (,) tilde (~) exclamation point (!) at sign (@) number sign (#) dollar sign ($) percent (%) caret (^) ampersand (&) apostrophe (') parenthesis (()) braces ({}) underscore (_) The following names are reserved and must not be used at the end of the naming scheme: -GATEWAY -GW -TAC Names must not start with a period (NetBIOS). Names must not be composed entirely of numbers (NetBIOS). Names must not contain a blank or space characters (DNS).

Required?	false
Default Value	

Accept Pipeline Input?	false

-NamingSchemeType<ADIdentityNamingScheme>

The type of naming scheme. This can be Numeric or Alphabetic. This defines the format of the variable part of the AD account names that will be created.

Required?	false
Default Value	Numeric
Accept Pipeline Input?	false

-OU<String>

The OU that computer accounts will be created into. If this is not specified, accounts are created into the default account container specified by AD. This is the 'Computers' container for out-of-the-box installations of AD. The OU must be a valid AD container and of the domain specified for the pool;

Required?	false
Default Value	
Accept Pipeline Input?	false

-Domain<String>

The AD domain name for the pool. Specify this in FQDN format; for example, MyDomain.com.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AllowUnicode<SwitchParameter>

Allow the naming scheme to have characters other than alphanumeric characters.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartCount<Int32>

Defines the next number that will be used if creating new AD accounts for the identity pool.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Scope<String[]>

The administration scopes to be applied to the new identity pool.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.IdentityPool

This object provides details of the identity pool and contains the following information:

IdentityPoolName <string>

The name of the identity pool.

IdentityPoolUid <Guid>

The unique identifier for the identity pool.

NamingScheme <string>

The naming scheme for the identity pool.

NamingSchemeType <Citrix.XDInterServiceTypes.ADIdentityNamingScheme>

The naming scheme type for the identity pool. This can be one of the following:

Numeric - naming scheme uses numeric indexes

Alphabetic - naming scheme uses alphabetic indexes

StartCount <int>

The next index to be used when creating an identity from the identity pool.

OU <string>

The Active Directory distinguished name for the OU in which accounts created from this identity pool will be created.

Domain <string>

The Active Directory domain that accounts in the pool belong to.

Lock <Boolean>

Indicates if the identity pool is locked.

Notes

In the case of failure, the following errors can result.

Error Codes

UnableToConvertDomainName

Unable to convert domain name to DNS format.

NamingSchemeNotEnoughCharacters

Naming scheme does not have enough characters specified.

NamingSchemeTooManyCharacters

Naming scheme has too many characters specified.

NamingSchemeIllegalCharacter

Naming scheme contains illegal characters.

NamingSchemeMayNotStartWithPeriod

Naming scheme starts with a period (.) character.

NamingSchemeMayNotBeAllNumbers

Naming scheme contains only numbers.

NamingSchemeMissingNumericSpecifications

Naming scheme does not contain any variable specification (i.e. no '#' characters are specified).

NamingSchemeHasMoreThanOneSetOfHashes

Naming scheme has more than one variable region (i.e. there are '#' characters separated by other characters).

IdentityPoolDuplicateObjectExists

An identity pool with the same name already exists.

IdentityPoolOUInvalid

Identity Pool OU invalid as it does not exist.

IdentityPoolOUOfWrongDomain

IdentityPool OU invalid as it refers to a different domain to the domain specified for the pool.

InvalidIdentityPoolParameterCombination

Caused by either of the following validation errors:

* If an OU is specified then a domain must also be specified.

* NamingScheme, NamingSchemeType and Domain must all be present if any of these are specified.

NamingSchemeIllegalComputerName

The naming scheme supplied is not valid.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>New-AcctIdentityPool -IdentityPoolName MyPool -NamingScheme Acc#### -Domain MyDomain.com -NamingSchemeType Numeric


IdentityPoolName : MyPool
IdentityPoolUid  : 22072d9e-6a8f-494b-a5bc-2ef18ca4b915
NamingScheme     : Acc####
NamingSchemeType : Numeric
StartCount       : 1
OU               :
Domain           : MyDomain.com
Lock             : False
```

Create a new identity pool from which accounts can be created in the domain called "MyDomain.com" using a numeric scheme of the format Acc####. The first account that will be created from this identity pool definition is Acc0001.

New AD accounts can be imported into this pool too, but must be from the Domain "MyDomain.com".

Remove-AcctADAccount

Sep 10, 2014

Removes AD computer accounts from an identity pool.

Syntax

Remove-AcctADAccount [-IdentityPoolName] <String> -ADAccountName <String[]> [-RemovalOption <ADIdentityRemoveAccountOption>] [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctADAccount [-IdentityPoolName] <String> -ADAccountSid <String[]> [-RemovalOption <ADIdentityRemoveAccountOption>] [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctADAccount -IdentityPoolUid <Guid> -ADAccountSid <String[]> [-RemovalOption <ADIdentityRemoveAccountOption>] [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctADAccount -IdentityPoolUid <Guid> -ADAccountName <String[]> [-RemovalOption <ADIdentityRemoveAccountOption>] [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to remove AD accounts from an identity pool. This removes the AD account from the Citrix service management scope. This process provides the options for removing the account in AD (or disabling it) if required.

All aspects of this command that need to make modifications to the accounts in AD will use the account that the runspace is using. This means that if an account is to be removed from AD or disabled, the user performing the operation in PowerShell must have sufficient privileges in AD for this operation to complete successfully.

If the option to remove the account from AD or to disable it in AD is specified, the AD operation must succeed for the account to be removed from the Citrix AD Identity Service database. Use caution when using the Force parameter because this allows removal of accounts that are in the 'inUse' state, which may result in the machines becoming unusable.

Related topics

New-AcctADAccount

Add-AcctADAccount

Repair-AcctADAccount

Unlock-AcctADAccount

Update-AcctADAccount

Get-AcctADAccount

Parameters

-IdentityPoolName<String>

The identity pool that the accounts are to be removed from.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ADAccountName<String[]>

The AD account name to be removed. AD accounts are accepted in the following formats: Fully qualified DN e.g. CN=MyComputer,OU=Computers,DC=MyDomain,DC=Com; UPN format e.g MyComputer@MyDomain.Com; Domain qualified e.g MyDomain\MyComputer.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ADAccountSid<String[]>

The Active Directory Account SID for the account to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IdentityPoolUid<Guid>

The unique identifier for the identity pool that the accounts are to be removed from.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-RemovalOption<ADIdentityRemoveAccountOption>

Defines the behavior relating to the AD account.

None - Do not attempt to remove the account from AD Delete - Attempt to remove the account from AD Disable - Attempt to disable the account in AD

Required?	false
Default Value	None
Accept Pipeline Input?	false

-Force<SwitchParameter>

Indicates if accounts that are marked as 'in-use' can be removed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.AccountOperationSummary

The remove-AcctADAccout command returns an object with the following parameters;

SuccessfulAccountsCount <int>

The number of accounts that were removed successfully.

FailedAccountsCount <int>

The number of accounts that were not removed.

FailedAccounts <Citrix.AdIdentity.Sdk.AccountError[]>

The list of accounts that failed to be removed. Each one has the following parameters:

ADAccountName <string>

ADAccountSid <String>

ErrorReason <AdIdentityStatus>

This can be one of the following

UnableToConvertDomain

IdentityNotLocatedInDomain

IdentityNotInIdentityPool

IdentityObjectInUse

IdentityObjectLocked

ADServiceDatabaseError

ADServiceDatabaseNotConfigured

ADServiceStatusInvalidDb

FailedToConnectToDomainController

FailedToDisableAccountInAD

FailedToDeleteAccountInAD

FailedToExecuteSearchInAD

FailedToAccessComputerAccountInAD

DiagnosticInformtion <Exception>

Any other error information

Notes

In the case of failure, the following errors can result.

Error Codes

IdentityPoolNotFound

The specified identity pool was not found.

IdentityPoolAlreadyLocked

The specified identity pool was locked by another operation.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Remove-AcctADAccount -IdentityPool MyPool -ADAccountName "Domain\account","domain\account2"


   SuccessfulAccountsCount     FailedAccountsCount   FailedAccounts
   -----------------------     -------------------   --------------
                 2                 0   {}
```

Removes two accounts (account and account2) from the identity pool called "MyPool", leaving the AD accounts untouched.

-------------------------- EXAMPLE 2 --------------------------

```
C:\PS>Remove-AcctADAccount -IdentityPool MyPool -RemovalOption Delete -ADAccountName "Domain\account","domain\account2"


   SuccessfulAccountsCount      FailedAccountsCount    FailedAccounts
   -----------------------      -------------------    --------------
                 2                  0   {}
```

Removes two accounts (account and account2) from the identity pool called "MyPool" (and from Active Directory).

-------------------------- EXAMPLE 3 --------------------------

```
C:\PS>Remove-AcctADAccount -IdentityPool MyPool -ADAccountName "Domain\account","domain\account2" -Force


   SuccessfulAccountsCount      FailedAccountsCount    FailedAccounts
   -----------------------      -------------------    --------------
                 2                  0   {}
```

Removes two accounts (account and account2) from the identity pool called "MyPool", leaving the AD accounts untouched. The accounts are removed regardless of whether they are in the 'inUse' state or not.

-------------------------- EXAMPLE 4 --------------------------

```
C:\PS>Remove-AcctADAccount -IdentityPool MyPool -ADAccountName "Domain\account","domain\account2" -OutVariable result

   SuccessfulAccountsCount      FailedAccountsCount    FailedAccounts
   -----------------------      -------------------    --------------
   1                            1   {account2}

   C:\PS>$result[0].FailedAccounts

   ADAccountName              ADAccountSid         ErrorReason
   -------------              -------------        ------------
   Domain\account2            account2             IdentityObjectLocked
```

Shows failure of removal of one of two accounts and how to retrieve the failure reason.

-------------------------- EXAMPLE 5 --------------------------

```
C:\PS>Remove-AcctADAccount -IdentityPool MyPool -ADAccountSid S-1-5-21-1315084875-1285793635-2418178940-2685


   SuccessfulAccountsCount      FailedAccountsCount    FailedAccounts
   -----------------------      -------------------    --------------
   1                            0   {}
```

Removes one account (S-1-5-21-1315084875-1285793635-2418178940-2685) from the identity pool called "MyPool", leaving the AD accounts untouched.

Remove-AcctIdentityPool

Sep 10, 2014

Removes identity pools.

Syntax

```
Remove-AcctIdentityPool [-IdentityPoolName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctIdentityPool -IdentityPoolUid <Guid> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove identity pools. The identity pool must be emptied of any AD accounts that it contains before it can be removed.

Related topics

New-AcctIdentityPool

Rename-AcctIdentityPool

Set-AcctIdentityPool

Unlock-AcctIdentityPool

Parameters

-IdentityPoolName<String>

The name of the identity pool to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IdentityPoolUid<Guid>

The unique identifier for the identity pool to remove.

Required?	true
Default Value	

Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

In the case of failure the following errors can be produced.

Error Codes

IdentityPoolObjectNotFound

The specified identity pool could not be located.

UnableToRemoveDueToAssociatedAccounts

The identity pool is not empty.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\Remove-AcctIdentityPool -IdentityPoolName MyPool
```

Removes the identity pool called "MyPool".

Remove-AcctIdentityPoolMetadata

Sep 10, 2014

Removes metadata from the given IdentityPool.

Syntax

Remove-AcctIdentityPoolMetadata [-IdentityPoolUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctIdentityPoolMetadata [-IdentityPoolUid] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctIdentityPoolMetadata [-IdentityPoolName] <String> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctIdentityPoolMetadata [-IdentityPoolName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctIdentityPoolMetadata [-InputObject] <IdentityPool[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctIdentityPoolMetadata [-InputObject] <IdentityPool[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to remove metadata from the given IdentityPool.

Related topics

Set-AcctIdentityPoolMetadata

Parameters

-IdentityPoolUid<Guid>

Id of the IdentityPool

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-IdentityPoolName<String>

Name of the IdentityPool

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<IdentityPool[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-

LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AcctIdentityPool | % { Remove-AcctIdentityPoolMetadata -Map $_.MetadataMap }
```

Remove all metadata from all IdentityPool objects.

Remove-AcctIdentityPoolScope

Sep 10, 2014

Remove the specified IdentityPool(s) from the given scope(s).

Syntax

```
Remove-AcctIdentityPoolScope [-Scope] <String[]> -InputObject <IdentityPool[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctIdentityPoolScope [-Scope] <String[]> -IdentityPoolUid <Guid[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctIdentityPoolScope [-Scope] <String[]> -IdentityPoolName <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The RemoveAcctIdentityPoolScope cmdlet is used to remove one or more IdentityPool objects from the given scope(s).

There are multiple parameter sets for this cmdlet, allowing you to identify the IdentityPool objects in different ways:

- IdentityPool objects can be piped in or specified by the InputObject parameter

- The IdentityPoolUid parameter specifies objects by IdentityPoolUid

- The IdentityPoolName parameter specifies objects by IdentityPoolName (supports wildcards)

To remove a IdentityPool from a scope you need permission to change the scopes of the IdentityPool.

If the IdentityPool is not in a specified scope, that scope will be silently ignored.

Related topics

Add-AcctIdentityPoolScope

Get-AcctScopedObject

Parameters

-Scope<String[]>

Specifies the scopes to remove the objects from.

Required?	true
Default Value	
Accept Pipeline Input?	false

-InputObject<IdentityPool[]>

Specifies the IdentityPool objects to be removed.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-IdentityPoolUid<Guid[]>

Specifies the IdentityPool objects to be removed by IdentityPoolUid.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-IdentityPoolName<String[]>

Specifies the IdentityPool objects to be removed by IdentityPoolName.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

None

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

ScopeNotFound

One of the specified scopes was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command with the specified objects or scopes.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

c:\PS>Remove-AcctIdentityPoolScope Finance -IdentityPoolUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
Removes a single IdentityPool from the 'Finance' scope.

-------------------------- EXAMPLE 2 --------------------------

c:\PS>Remove-AcctIdentityPoolScope Finance,Marketing -IdentityPoolUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
Removes a single IdentityPool from multiple scopes.

---------- EXAMPLE 3 ----------

c:\PS>Get-AcctIdentityPool | Remove-AcctIdentityPoolScope Finance
Removes all visible IdentityPool objects from the 'Finance' scope.

---------- EXAMPLE 4 ----------

c:\PS>Remove-AcctIdentityPoolScope Finance -IdentityPoolName A*
Removes IdentityPool objects with a name starting with an 'A' from the 'Finance' scope.

Remove-AcctServiceMetadata

Sep 10, 2014

Removes metadata from the given Service.

Syntax

```
Remove-AcctServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctServiceMetadata [-ServiceHostId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctServiceMetadata [-InputObject] <Service[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AcctServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Service.

Related topics

Set-AcctServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- **EXAMPLE 1** ----------

```
c:\PS>Get-AcctService | % { Remove-AcctServiceMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Service objects.

Rename-AcctIdentityPool

Sep 10, 2014

Renames an identity pool.

Syntax

Rename-AcctIdentityPool [-IdentityPoolName] <String> [-NewIdentityPoolName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-AcctIdentityPool -IdentityPoolUid <Guid> -NewIdentityPoolName <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to change the name of an existing identity pool.

Related topics

Get-AcctIdentityPool

Set-AcctIdentityPool

Remove-AcctIdentityPool

Test-AcctIdentityPoolNameAvailable

Parameters

-IdentityPoolName<String>

The name of the identity pool to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IdentityPoolUid<Guid>

The unique identifier for the identity pool to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	false

-NewIdentityPoolName<String>

The new name for the identity pool. This must be a name which is not used by an existing identity pool, and it must not contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

Defines whether or not the command returns a result showing the new state of the updated provisioning scheme.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.IdentityPool

This object provides details of the identity pool and contains the following information:

IdentityPoolName <string>

The name of the identity pool.

IdentityPoolUid <Guid>

The unique identifier for the identity pool.

NamingScheme <string>

The naming scheme for the identity pool.

NamingSchemeType <Citrix.XDInterServiceTypes.ADIdentityNamingScheme>

The naming scheme type for the identity pool. This can be one of the following:

Numeric - naming scheme uses numeric indexes

Alphabetic - naming scheme uses alphabetic indexes

StartCount <int>

The next index to be used when creating an identity from the identity pool.

OU <string>

The Active Directory distinguished name for the OU in which accounts created from this identity pool will be created.

Domain <string>

The Active Directory domain that accounts in the pool belong to.

Lock <Boolean>

Indicates if the identity pool is locked.

Notes

In the case of failure the following errors can result.

Error Codes

IdentityPoolObjectNotFound

The specified identity pool could not be located.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

C:\PS>Rename-AcctIdentityPool -IdentityPoolName oldName -NewIdentityPoolName newName
Renames an existing identity pool called "oldName" to be called "newName".

Repair-AcctADAccount

Sep 10, 2014

Resets the Active Directory machine password for the given accounts.

Syntax

```
Repair-AcctADAccount -ADAccountName <String[]> [-Password <String>] [-SecurePassword <SecureString>] [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Repair-AcctADAccount -ADAccountSid <String[]> [-Password <String>] [-SecurePassword <SecureString>] [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This provides the ability to synchronize the account password stored in Active Directory with the password stored in the AD Identity Service. If successful, this results in the AD Identity Service account state being reset to 'available' so it can be consumed by other Machine Creation Services.

If the current account password is not suplied using the Password or SecurePassword Parameters, this requires the user who initiated the runspace to have the required permissions in Active Directory to reset the Active Directory Account password.

If the current account password is supplied then this command will use the password change operation which does not require any elevated permissions in Active Directory.

Related topics

New-AcctADAccount

Add-AcctADAccount

Remove-AcctADAccount

Unlock-AcctADAccount

Update-AcctADAccount

Get-AcctADAccount

Parameters

-ADAccountName<String[]>

The Active Directory account name(s) that are to be repaired. Active Directory accounts are accepted in the following formats: Fully qualified DN e.g. CN=MyComputer,OU=Computers,DC=MyDomain,DC=Com; UPN format e.g MyComputer@MyDomain.Com; Domain qualified e.g MyDomain\MyComputer.

Required?	true
Default Value	

Accept Pipeline Input?	false

-ADAccountSid<String[]>

The Active Directory account SID(s) that are to be repaired.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Password<String>

The current password for the computer account.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecurePassword<SecureString>

The current password for the account (provided in a Secure String class).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

Indicates whether accounts that are marked as 'in-use' can be repaired or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.AccountOperationSummary

The Repair-AcctADAccout command returns an object with the following parameters:

SuccessfulAccountsCount <int>

The number of accounts that were repaired successfully.

FailedAccountsCount <int>

The number of accounts that were not repaired.

FailedAccounts <Citrix.AdIdentity.Sdk.AccountError[]>

The list of accounts that failed to be repaired. Each one has the following parameters:

ADAccountName <string>

ADAccountSid <String>

ErrorReason <AdIdentityStatus>

This can be one of the following

UnableToConvertDomain

IdentityNotLocatedInDomain

IdentityNotFound

IdentityObjectInUse

IdentityObjectLocked

ADServiceDatabaseError

ADServiceDatabaseNotConfigured

ADServiceStatusInvalidDb

FailedToConnectToDomainController

FailedToExecuteSearchInAD

FailedToAccessComputerAccountInAD

FailedToSetPasswordInAD

FailedToChangePasswordInAD

DiagnosticInformtion <Exception>

Any other error information

Notes

In the case of failure, the following errors can result.

Error Codes

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Repair-AcctADAccount -ADAccountName "Domain\account","domain\account2"


    SuccessfulAccountsCount     FailedAccountsCount   FailedAccounts
    -----------------------     -------------------   --------------
                  2                   0   {}
```

Reset-AcctServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the AdIdentity Service.

Syntax

```
Reset-AcctServiceGroupMembership [-ConfigServiceInstance] <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables you to reload AdIdentity Service access permissions and configuration service locations. The Reset-AcctServiceGroupMembership command must be run on at least one instance of the service type (Acct) after installation and registration with the configuration service. Without this operation, the AdIdentity services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-AcctServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Parameters

-ConfigServiceInstance<ServiceInstance[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.AdIdentity.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-AcctServiceGroupMembership command.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-AcctServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-AcctServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Set-AcctDBConnection

Sep 10, 2014

Configures a database connection for the AdIdentity Service.

Syntax

```
Set-AcctDBConnection [-DBConnection] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Configures a connection to a database in which the AdIdentity Service can store its state. The service will attempt to connect and start using the database immediately after the connection is configured. The database connection string is updated to the specified value regardless of whether it is valid or not. Specifying an invalid connection string prevents a service from functioning until the error is corrected.

After a connection is configured, you cannot alter it without first clearing it (by setting the connection to $null).

You do not need to configure a database connection to use this command.

Related topics

Get-AcctServiceStatus

Get-AcctDBConnection

Test-AcctDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the AdIdentity Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-AcctDBConnection command returns an object containing the status of the AdIdentity Service together with extra diagnostics information.

DBUnconfigured

The AdIdentity Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the AdIdentity Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the AdIdentity Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the AdIdentity Service currently in use is incompatible with the version of the AdIdentity Service schema on the database. Upgrade the AdIdentity Service to a more recent version.

DBOlderVersionThanService

The version of the AdIdentity Service schema on the database is incompatible with the version of the AdIdentity Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The AdIdentity Service is running and is connected to a database containing a valid schema.

Failed

The AdIdentity Service has failed.

Unknown

The status of the AdIdentity Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Set-AcctDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Configures a database connection string for the AdIdentity Service.

-------------------------- EXAMPLE 2 --------------------------

```
c:\PS>Set-AcctDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Configures an invalid database connection string for the AdIdentity Service.

Set-AcctIdentityPool

Sep 10, 2014

Update parameters of an identity pool.

Syntax

Set-AcctIdentityPool [-IdentityPoolName] <String> [-NamingScheme <String>] [-NamingSchemeType <ADIdentityNamingScheme>] [-OU <String>] [-Domain <String>] [-AllowUnicode] [-PassThru] [-StartCount <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AcctIdentityPool -IdentityPoolUid <Guid> [-NamingScheme <String>] [-NamingSchemeType <ADIdentityNamingScheme>] [-OU <String>] [-Domain <String>] [-AllowUnicode] [-PassThru] [-StartCount <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to modify the parameters of an identity pool.

Note: When changing a naming scheme or naming scheme type, the index is not reset to 0; it continues to avoid AD account name clashes with existing accounts. If required, use the New-AcctAdAccount command to change the index when creating further accounts.

Related topics

New-AcctIdentityPool

Get-AcctIdentityPool

Remove-AcctIdentityPool

Parameters

-IdentityPoolName<String>

The name of the identity pool that is to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IdentityPoolUid<Guid>

The unique identifier for the identity pool that is to be updated.

Required?	true

Default Value	
Accept Pipeline Input?	false

-NamingScheme<String>

The new naming scheme that is to be used for the identity pool.

Required?	false
Default Value	
Accept Pipeline Input?	false

-NamingSchemeType<ADIdentityNamingScheme>

The new naming scheme type that is to be used for the identity pool. This can be Numeric or Alphabetic.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OU<String>

The new OU to be used for the Identity Pool. All accounts created after this is set are created in this AD container. This will not move any of the existing accounts. The OU must be a valid AD container and of the domain specified for the pool.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Domain<String>

The new Active Directory domain that is to be used for the identity pool. All new accounts will be created in this domain, but this will not impact any of the existing accounts. The domain can be specified in either long or short form (i.e. domain or domain.com).

Required?	false

Default Value	
Accept Pipeline Input?	false

-AllowUnicode<SwitchParameter>

Updates the definition of the allowed characters in a naming scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Defines whether the command returns the new state of the identity pool or not.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-StartCount<Int32>

The start index for the next create operation

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.AdIdentity.Sdk.IdentityPool

This object provides details of the identity pool and contains the following information:

IdentityPoolName <string>

The name of the identity pool.

IdentityPoolUid <Guid>

The unique identifier for the identity pool.

NamingScheme <string>

The naming scheme for the identity pool.

NamingSchemeType <Citrix.XDInterServiceTypes.ADIdentityNamingScheme>

The naming scheme type for the identity pool. This can be one of the following:

Numeric - naming scheme uses numeric indexes

Alphabetic - naming scheme uses alphabetic indexes

StartCount <int>

The next index to be used when creating an identity from the identity pool.

OU <string>

The Active Directory distinguished name for the OU in which accounts created from this identity pool will be created.

Domain <string>

The Active Directory domain that accounts in the pool belong to.

Lock <Boolean>

Indicates whether the identity pool is locked.

Notes

In the case of failure, the following errors can result.

Error Codes

InvalidIdentityPoolParameterCombination

Caused by either of the following validation errors:

* If an OU is specified then a domain must also be specified.

* NamingScheme, NamingSchemeType and Domain must all be present if any of them are specified.

NamingSchemeIllegalComputerName

The naming scheme supplied is not valid.

UnableToConvertDomainName

Unable to convert domain name to DNS format.

NamingSchemeNotEnoughCharacters

Naming scheme does not have enough characters specified.

NamingSchemeTooManyCharacters

Naming scheme has too many characters specified.

NamingSchemeIllegalCharacter

Naming scheme contains illegal characters.

NamingSchemeMayNotStartWithPeriod

Naming scheme starts with a period (.) character.

NamingSchemeMayNotBeAllNumbers

Naming scheme contains only numbers.

NamingSchemeMissingNumericSpecifications

Naming scheme does not contain any variable specification (i.e. no '#' characters are specified).

NamingSchemeHasMoreThanOneSetOfHashes

Naming scheme has more than one variable region (i.e. there are '#' characters separated by other characters).

IdentityPoolDuplicateObjectExists

An identity pool with the same name exists already.

IdentityPoolObjectNotFound

The identity pool to be modified could not be located.

IdentityPoolOUInvalid

Identity Pool OU invalid as it does not exist.

IdentityPoolOUOfWrongDomain

IdentityPool OU invalid as it refers to a different domain to the domain specified for the pool.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Set-AcctIdentityPool -IdentityPoolName poolName -StartCount 100 -NamingScheme AC####
```


Changes the start count, and the naming scheme, so that the next account generated will be AC0100 (assuming that account does not already exist)

Set-AcctIdentityPoolMetadata

Sep 10, 2014

Adds or updates metadata on the given IdentityPool.

Syntax

Set-AcctIdentityPoolMetadata [-IdentityPoolUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AcctIdentityPoolMetadata [-IdentityPoolUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AcctIdentityPoolMetadata [-IdentityPoolName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AcctIdentityPoolMetadata [-IdentityPoolName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AcctIdentityPoolMetadata [-InputObject] <IdentityPool[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AcctIdentityPoolMetadata [-InputObject] <IdentityPool[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given IdentityPool objects.

Related topics

Remove-AcctIdentityPoolMetadata

Parameters

-IdentityPoolUid<Guid>

Id of the IdentityPool

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-IdentityPoolName<String>

Name of the IdentityPool

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<IdentityPool[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the IdentityPool specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-AcctIdentityPoolMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-AcctIdentityPoolMetadata -IdentityPoolUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

    Key                            Value
    ---                            -----
    property                           value
```

Add metadata with a name of 'property' and a value of 'value' to the IdentityPool with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-AcctServiceMetadata

Sep 10, 2014

Adds or updates metadata on the given Service.

Syntax

Set-AcctServiceMetadata [-ServiceHostId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AcctServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AcctServiceMetadata [-InputObject] <Service[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AcctServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Allows you to store additional custom data against given Service objects.

Related topics

Remove-AcctServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Service specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-AcctServiceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Set-AcctServiceMetadata -ServiceHostId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Service with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Test-AcctDBConnection

Sep 10, 2014

Tests a database connection for the AdIdentity Service.

Syntax

```
Test-AcctDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Tests a connection to the database in which the AdIdentity Service can store its state. The service will attempt to connect to the database without affecting the current connection to the database.

You do not have to clear the connection to use this command.

Related topics

Get-AcctServiceStatus

Get-AcctDBConnection

Set-AcctDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the AdIdentity Service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-AcctDBConnection command returns an object containing the status of the AdIdentity Service if the connection string of the specified data store were to be set to the string being tested, together with extra diagnostics information for the specified connection string.

DBRejectedConnection

The database rejected the logon attempt from the AdIdentity Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the AdIdentity Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the AdIdentity Service currently in use is incompatible with the version of the AdIdentity Service schema on the database. Upgrade the AdIdentity Service to a more recent version.

DBOlderVersionThanService

The version of the AdIdentity Service schema on the database is incompatible with the version of the AdIdentity Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Set-AcctDBConnection command would succeed if it were executed with the supplied connection string.

Failed

The AdIdentity Service has failed.

Unknown

The status of the AdIdentity Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Test-AcctDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"
```


OK
Tests a database connection string for the AdIdentity Service.

---------- EXAMPLE 2 ----------

c:\PS>Test-AcctDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
Tests an invalid database connection string for the AdIdentity Service.

Test-AcctIdentityPoolNameAvailable

Sep 10, 2014

Checks to ensure that the proposed name for an identity pool is unused.

Syntax

```
Test-AcctIdentityPoolNameAvailable [-IdentityPoolName] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Checks to ensure that the proposed name for an identity pool is unused. This check is done without regard for scoping of existing identity pools, so the names of inaccessible pools are also checked.

Related topics

New-AcctIdentityPool

Rename-AcctIdentityPool

Parameters

-IdentityPoolName<String[]>

The name or names of the identity pool(s) to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

object[]

An array of PSObjects that pair the name and availability of the name

Notes

In the case of failure, the following errors can result.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
Test-AcctIdentityPoolNameAvailable -IdentityPoolName $NewPoolName
```

This tests whether the value of $NewPoolName is unique or not, and can be used to create a new provisioning scheme or rename an existing one without failing. True is returned if the name is good.

Unlock-AcctADAccount

Sep 10, 2014

Unlocks AD accounts within the AD Identity Service.

Syntax

```
Unlock-AcctADAccount -ADAccountName <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]

Unlock-AcctADAccount -ADAccountSid <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Provides the ability to unlock the AD Identity Service identity item that references a specified AD account. An AD account is marked as locked in the AD Identity Service while the Machine Creation Services (MCS) are processing tasks relating to the account. If these tasks are forcibly stopped, an account can remain locked despite no longer being processed. This command resolves this issue, but use it with caution because unlocking an account that MCS expects to be locked can result in an MCS operation being cancelled. Use this command only when MCS has locked an account for use in a provisioning operation, and where this operation has failed without unlocking the account.

Note: This command does NOT make any changes to the account information stored in Active Directory.

Related topics

Get-AcctADAccount

New-AcctADAccount

Add-AcctADAccount

Repair-AcctADAccount

Remove-AcctADAccount

Update-AcctADAccount

Unlock-AcctADAccount

Parameters

-ADAccountName<String>

The AD account name to be unlocked. AD account name is accepted in the following formats: Fully qualified DN e.g. CN=MyComputer,OU=Computers,DC=MyDomain,DC=Com; UPN format e.g MyComputer@MyDomain.Com; Domain qualified e.g MyDomain\MyComputer.

Required?	true
Default Value	

Accept Pipeline Input?	false

-ADAccountSid<String>

The AD account SID that represents the account to be unlocked.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.AdIdentity.Sdk.IdentityInPool You can pipe an object containing a parameter called 'ADAccountSID' to unlock-AcctADAccount.

Notes

In the case of failure, the following errors can result.

Error Codes

IdentityNotLocatedInDomain

The specified AD account could not be located in Active Directory.

IdentityObjectNotFound

The identity could not be found.

IdentityAlreadyUnlocked

The identity is not locked.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Unlock-AcctADAccount -ADAccountName Domain\account
```

Unlocks the AD account called "Domain\account".

---------- EXAMPLE 2 ----------

```
c:\PS>Get-AcctADAccount -Filter {lock -eq $true} | Unlock-AcctADAccount
```

Unlocks all the locked AD accounts.

Unlock-AcctIdentityPool

Sep 10, 2014

Unlocks identity pools.

Syntax

```
Unlock-AcctIdentityPool [-IdentityPoolName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Unlock-AcctIdentityPool -IdentityPoolUid <Guid> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to unlock the specified identity pool. Identity pools are locked automatically when being updated (e.g. when new accounts are being created into them). The pool must never be left in a locked state; this command allows recovery from an error should this ever occur. Use this command with caution, as unlocking an identity pool which is supposed to be locked may result in unexpected behavior.

Related topics

New-AcctIdentityPool

Remove-AcctIdentityPool

Set-AcctIdentityPool

Parameters

-IdentityPoolName<String>

The name of the identity pool to unlock.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IdentityPoolUid<Guid>

The unique identifier for the identity pool to be unlocked.

Required?	true
Default Value	

Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.AdIdentity.Sdk.IdentityPool You can pipe an object containing a parameter called 'IdentityPoolName' to unlock-AcctIdentityPool.

Notes

In the case of failure, the following errors can result.

Error Codes

IdentityPollObjectNotFound

The specified identity pool could not be located.

IdentityPoolAlreadyUnlocked

The specified identity pool is not locked.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Unlock-AcctIdentityPool -IdentityPool MyPool
```
Unlocks the identity pool called "MyPool".

---------- EXAMPLE 2 ----------

```
C:\PS>Get-AcctIdentityPool -Filter {Lock -eq $true} | Unlock-AcctIdentityPool
```
Unlocks all the locked identity pools.

Update-AcctADAccount

Sep 10, 2014

Refreshes the AD computer account state stored in the AD Identity Service.

Syntax

Update-AcctADAccount [-IdentityPoolName] <String> [-AllAccounts] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Update-AcctADAccount -IdentityPoolUid <Guid> [-AllAccounts] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to synchronize the state of the AD accounts stored in the AD Identity Service with the AD accounts themselves. By default, this checks all accounts marked as 'error' to determine if accounts are still in an error state (i.e. disabled or locked). If you specify the 'AllAccounts' option, it checks accounts not in error state and updates the status of these accounts too.

Related topics

New-AcctADAccount

Add-AcctADAccount

Remove-AcctADAccount

Repair-AcctADAccount

Unlock-AcctADAccount

Get-AcctADAccount

Parameters

-IdentityPoolName<String>

The name of the identity pool for the accounts to be refreshed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IdentityPoolUid<Guid>

The unique identifier for the identity pool of the AD accounts that are to be refreshed.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AllAccounts<SwitchParameter>

Indicates if all accounts should be refreshed or only the ones marked as in error.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

In the case of failure, the following errors can result.

Error Codes

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Update-AcctADAccount -IdentityPoolName MyPool
```

Checks the status of all accounts in the Identity Pool MyPool that are currently mark as in the Error state and checks if the account is now available.

---------- EXAMPLE 2 ----------

```
c:\PS>Update-AcctADAccount -IdentityPoolName MyPool -AllAccounts
```

Checks the status of all accounts in the Identity Pool MyPool marking them as Available, InUse, Tainted or Error as appropriate.

Citrix.AppV.Admin.V1

Sep 10, 2014

Cmdlets

Name	Description
ConvertTo-CtxAppVLauncherArg	Returns a string containing information to send to the App-V Launcher. You can plug this string directly into the Virtual Delivery Agent (VDA) to launch App-V applications.
Get-CtxAppVApplication	Enumerates all published App-V applications for a given Management server.
Get-CtxAppVApplicationInfo	Enumerates information for a given application in a given package for a given Management server.
Get-CtxAppVServer	Returns URLs for App-V Publishing and Management servers contained in a Citrix App-V policy. Returned values are in string format.
Get-CtxAppVServerSetting	Returns settings for the specified App-V Publishing Server.
New-CtxAppVServer	Creates a new Citrix App-V policy containing the specified App-V Management and Publishing Server URLs.
Set-CtxAppVServerSetting	Specifies the App-V Publishing server settings to use on the VDA. These settings determine whether or not the App-V Client can automatically initiate a publishing refresh on certain events such as user logon or at specified intervals.
Test-CtxAppVServer	Tests the given URL for the presence of App-V Management and Publishing servers.

ConvertTo-CtxAppVLauncherArg

Sep 10, 2014

Returns a string containing information to send to the App-V Launcher. You can plug this string directly into the Virtual Delivery Agent (VDA) to launch App-V applications.

Syntax

ConvertTo-CtxAppVLauncherArg [-AppVPublishingServer] <string> [[-PackageId] <String>] [-AppId] <String> -SeqLoc <String> -TargetInPackage <boolean> [<CommonParameters>]

ConvertTo-CtxAppVLauncherArg [-LauncherPath] <SwitchParameter> [<CommonParameters>]

Detailed Description

Returns a string containing information to send to the App-V Launcher. You can plug this string directly into the Virtual Delivery Agent (VDA) to launch App-V applications.

Related topics

Parameters

-AppVPublishingServer<>

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-PackageId<>

The Package Id of the application.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AppId<>

The App Id of the application.

Required?	True
Default Value	
Accept Pipeline Input?	false

-SeqLoc<>

The sequence location of the package.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetInPackage<>

Pass this as $true if TargetInPackage field is "true" in the Manifest file for the particular App Id.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LauncherPath<>

Gets the Citrix Launcher path. The Citrix Launcher is a component installed on the VDA.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

Examples

---------- EXAMPLE 1 ----------

ConvertTo-CtxAppVLauncherArg -AppVPublishingServer "http://appv-2k82-srv.blrstrm.com:8082" -PackageId "1bcb6993-10b1-4659-b9d4-e809e10cecdf_5" -AppId "[{Progran
Converts the arguments provided into a cmdlet to launch Beyond Compare from http://appv-server on the VDA.

---------- EXAMPLE 2 ----------

ConvertTo-CtxAppVLauncherArg -LauncherPath
Gets the Citrix App-V Launcher path.

Get-CtxAppVApplication

Sep 10, 2014

Enumerates all published App-V applications for a given Management server.

Syntax

```
Get-CtxAppVApplication [-AppVManagementServer] <string> [<CommonParameters>]
```

Detailed Description

Queries a given Management server and fetches all published applications for that server. Applications that are published but have no user Entitlements are not displayed by this cmdlet.

Related topics

Parameters

-AppVManagementServer<String>

App-V Management Server

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

Examples

---------- EXAMPLE 1 ----------

```
Get-CtxAppVApplication -AppVManagementServer "xmas-demo-appv"
```

Displays all published applications for the Management server "xmas-demo-appv" .

Get-CtxAppVApplicationInfo

Sep 10, 2014

Enumerates information for a given application in a given package for a given Management server.

Syntax

Get-CtxAppVApplicationInfo [-AppVManagementServer] <string> [-AppId] <String> [-PackageID] <string> [[-Property] <string[]>] [<CommonParameters>]

Get-CtxAppVApplicationInfo [-AppVManagementServer] <String> [[-InputObject] <AppVServeApplications[]>] [[-Property] <string[]>] [<CommonParameters>]

Detailed Description

Queries a given Management server and fetches the requested information for a given application.

Related topics

Parameters

-AppvManagementServer<string>

Machine name of the App-V Management server. The name does not need to be specified as a Fully Qualified Domain Name (FQDN).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AppId<string>

The App Id of the given application.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PackageId<string>

The Package Id of the given application.

Required?	false
Default Value	
Accept Pipeline Input?	false

Return Values

Citrix.VirtApp.Studio.PowerShellManager.AppVAppData

Examples

---------- EXAMPLE 1 ----------

Get-CtxAppVApplicationInfo -AppVManagementServer "xmas-demo-appv" -AppId "[{ProgramFilesX86}]\Beyond Compare 3\BCompare.exe" -PackageId "1bcb6993-10b1-4659-
Fetches all application information for the Beyond Compare 3 application from the xmas-demo-appv Management server.

---------- EXAMPLE 2 ----------

Get-CtxAppVApplicationInfo -AppVManagementServer "xmas-demo-appv" -AppId "[{ProgramFilesX86}]\Beyond Compare 3\BCompare.exe" -PackageId "1bcb6993-10b1-4659-
Fetches only information about FTA and User Entitlements for the Beyond Compare 3 application from the xmas-demo-appv Management server.

---------- EXAMPLE 3 ----------

Get-CtxAppVApplication -AppVManagementServer "xmas-demo-appv" | Get-CtxAppVApplicationInfo -AppVManagementServer "xmas-demo-appv"
Pipelines the output of Get-CtxAppvApplication to Get-CtxAppvApplicationInfo to get the application properties of all the published applications on the xmas-demo-appv Management server.

Get-CtxAppVServer

Sep 10, 2014

Returns URLs for App-V Publishing and Management servers contained in a Citrix App-V policy. Returned values are in string format.

Syntax

```
Get-CtxAppVServer -ByteArray <byte[]> [-ConsumedByStudio <bool>] [<CommonParameters>]
```

Detailed Description

Returns URLs for App-V Publishing and Management servers contained in a Citrix App-V policy. Returned values are in string format.

Related topics

Parameters

-ByteArray<>

Specifies the Citrix App-V policy created using the New-CtxAppVServer cmdlet.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ConsumedByStudio<>

If set to "true", outputs URLs for the App-V Publishing and Management servers. If set to "false", outputs both the URL and settings for the App-V Publishing server.

Required?	false
Default Value	
Accept Pipeline Input?	false

Examples

---------- EXAMPLE 1 ----------

```
$config = Get-BrokerMachineConfiguration -Name appv*
Get-CtxAppVServer -ByteArray $config[0].Policy
```

Returns Publishing Server URL , Management Server URL configured in given policy

Get-CtxAppVServerSetting

Sep 10, 2014

Returns settings for the specified App-V Publishing Server.

Syntax

```
Get-CtxAppVServerSetting -AppVPublishingServer <string> [<CommonParameters>]
```

Detailed Description

Returns settings for the specified App-V Publishing Server. For more information about these settings, see the App-V documentation on the Microsoft website at http://technet.microsoft.com/en-us/library/jj687745.aspx

Related topics

Parameters

-AppVPublishingServer<>

URL of the Publishing Server for which settings are to be returned.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

Return Values

Publishing Server settings. These settings are : GlobalRefreshEnabled; GlobalRefreshOnLogon;GlobalRefreshInterval;GlobalRefreshIntervalUnit;UserRefreshEnabled; UserRefreshOnLogon;UserRefreshInterval;UserRefreshIntervalUnit;

Examples

---------- EXAMPLE 1 ----------

```
Get-CtxAppVServerSetting -AppVPublishingServer http://AppV50Publishing:8082
```

This example returns settings associated with http://AppV50PublishingServer:8082 in the following format:

GlobalRefreshEnabled: false

GlobalRefreshOnLogon: false

GlobalRefreshInterval: 0

GlobalRefreshIntervalUnit: Day

UserRefreshEnabled: true

```
UserRefreshOnLogon: false

UserRefreshInterval: 0

UserRefreshIntervalUnit: Hour
```

New-CtxAppVServer

Sep 10, 2014

Creates a new Citrix App-V policy containing the specified App-V Management and Publishing Server URLs.

Syntax

New-CtxAppVServer -PublishingServer <string> -ManagementServer <String> [-UserRefreshEnabled [<Boolean>]] [-UserRefreshOnLogon <Boolean>] [-UserRefreshInterval <int>] [-UserRefreshIntervalUnit <Enum>] [-GlobalRefreshEnabled [<Boolean>]] [-GlobalRefreshOnLogon <Boolean>] [-GlobalRefreshInterval <Int>] [-GlobalRefreshIntervalUnit <Enum>] [<CommonParameters>]

Detailed Description

Creates a new Citrix App-V policy containing the specified App-V Management and Publishing server URLs. Additionally, accepts Publishing Server settings that control how and when automatic refresh occurs on the VDA.

Related topics

Parameters

-PublishingServer<>

URL of the Publishing server to add to the Citrix policy.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ManagementServer<>

URL of the Management server to add to the Citrix policy.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-UserRefreshEnabled<>

Enables a refresh of packages published to user groups either at user logon or at a specified interval. For more information, see the App-V 5.0 documentation at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserRefreshOnLogon<>

Specifies whether or not to initiate a refresh of packages published to user groups on every user logon. For more information, see the App-V 5.0 documentation at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserRefreshInterval<>

Specifies the frequency at which to initiate a refresh of packages published to user groups. This can be either days or hours, as specified by the UserRefreshIntervalUnit setting. For more information, see the App-V 5.0 documentation at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	false
Default Value	

Accept Pipeline Input?	false

-UserRefreshInterval<>

Specifies the frequency at which to initiate a refresh of packages published to user groups. This can be either days or hours, as specified by the UserRefreshIntervalUnit setting. For more information, see the App-V 5.0 documentation at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserRefreshIntervalUnit<>

Specifies the unit for the UserRefreshInterval setting. This can be set to either Hours (0) or Days (1). For more information, see the App-V 5.0 documentation at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	false
Default Value	
Accept Pipeline Input?	false

-GlobalRefreshEnabled<>

Enables a refresh of packages published to machine groups either at user logon or at a specified interval. For more information, see the App-V 5.0 documentation at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	false
Default Value	
Accept Pipeline Input?	false

-GlobalRefreshOnLogon<>

Specifies whether or not to initiate a refresh of packages published to machine groups on every user logon. For more information, see the App-V 5.0 documentation at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	false
Default Value	
Accept Pipeline Input?	false

-GlobalRefreshInterval<>

Specifies the frequency at which to initiate a refresh of packages published to machine groups. This can be either days or hours, as specified by the GlobalRefreshIntervalUnit setting. Please refer to App-V 5.0 documentation for details. http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	false
Default Value	
Accept Pipeline Input?	false

-GlobalRefreshIntervalUnit<>

Specifies the unit for the GlobalRefreshInterval setting. This can be set to either Hours (0) or Days (1). Please refer to App-V 5.0 documentation for details. http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	false
Default Value	
Accept Pipeline Input?	false

Examples

---------- **EXAMPLE 1** ----------

New-CtxAppVServer -ManagementServer http://AppV-Mgmt-Server:8080 -PublishingServer http://appV-Pub-Server:8082
Creates a new Citrix Policy for Management Server AppV-Mgmt-Server:8080 & Publishing Server: AppV-Mgmt-Server:8082. Default Publishing Server setting is used for htttp://AppV-Mgmt-Server:8082

Default values for publishing server settings used for Http://AppV-Mgmt-Server:8082 are:

GlobalRefreshEnabled = false; GlobalLogonRefresh = false ; GlobalIntervalRefreshInterval = 0; GlobalIntervalRefreshUnit = Day

UserRefreshEnabled = true; UserLogonRefresh = true ; UserIntervalRefreshInterval = 0; GlobalIntervalRefreshUnit = Day

---------- **EXAMPLE 1** ----------

New-CtxAppVServer -ManagementServer http://AppV-Mgmt-Server:8080 -PublishingServer http://appV-Pub-Server:8082 -GlobalRefreshEnabled $true -GlobalLogonRefresh $t
Creates a new Citrix Policy for Management Server AppV-Mgmt-Server:8080 & Publishing Server: AppV-Mgmt-Server:8082. User specified Publishing Server settings are used for AppV-Mgmt-Server:8082

Following values are used to configure Publishing Server : http://AppV-Mgmt-Server:8082

GlobalRefreshEnabled = True; GlobalLogonRefresh = True ; GlobalIntervalRefreshInterval = 2; GlobalIntervalRefreshUnit = Hour

UserRefreshEnabled = true; UserLogonRefresh = true ; UserIntervalRefreshInterval = 3; GlobalIntervalRefreshUnit = Hour

Set-CtxAppVServerSetting

Sep 10, 2014

Specifies the App-V Publishing server settings to use on the VDA. These settings determine whether or not the App-V Client can automatically initiate a publishing refresh on certain events such as user logon or at specified intervals.

Syntax

```
Set-CtxAppVServerSetting -AppVPublishingServer <string> [-UserRefreshEnabled [<Boolean>]] [-UserRefreshOnLogon <Boolean>] [-UserRefreshInterval <int>] [-UserRefreshIntervalUnit <Enum>] [-GlobalRefreshEnabled [<Boolean>]] [-GlobalRefreshOnLogon <Boolean>] [-GlobalRefreshInterval <int>] [-GlobalRefreshIntervalUnit <Enum>] [<CommonParameters>]
```

Detailed Description

Specifies the App-V Publishing server settings to use on the VDA. These settings determine whether or not the App-V Client can automatically initiate a publishing refresh on certain events such as user logon or at specified intervals. Please refer to Microsoft App-V 5.0 documentation for more details on these settings : http://technet.microsoft.com/en-us/library/jj687745.aspx

Related topics

Parameters

-AppVPublishingServer<>

URL of the Publishing Server for which settings are to be set.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-UserRefreshEnabled<>

Enables a refresh of packages published to user groups either at user logon or at a specified interval. For more information, see the App-V documentation on the Microsoft website at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	True
Default Value	
Accept Pipeline Input?	false

-UserRefreshOnLogon<>

Specifies whether or not to initiate a refresh of packages published to user groups on every user logon. For more information, see the App-V documentation on the Microsoft website at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	true
Default Value	
Accept Pipeline Input?	false

-UserRefreshInterval<>

Specifies the frequency at which to initiate a refresh of packages published to user groups. This can be either days or hours, as specified by the UserRefreshIntervalUnit setting. For more information, see the App-V documentation on the Microsoft website at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	true
Default Value	
Accept Pipeline Input?	false

-UserRefreshIntervalUnit<>

Specifies the unit for the UserRefreshInterval setting. This can be set to either Hours (0) or Days (1). For more information, see the App-V documentation on the Microsoft website at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	true

Default Value	
Accept Pipeline Input?	false

-GlobalRefreshEnabled<>

Enables a refresh of packages published to machine groups either at user logon or at a specified interval. For more information, see the App-V documentation on the Microsoft website at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	True
Default Value	
Accept Pipeline Input?	false

-GlobalRefreshOnLogon<>

Specifies whether or not to initiate a refresh of packages published to machine groups on every user logon. For more information, see the App-V documentation on the Microsoft website at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	true
Default Value	
Accept Pipeline Input?	false

-GlobalRefreshInterval<>

Specifies the frequency at which to initiate a refresh of packages published to machine groups. This can be either days or hours, as specified by the GlobalRefreshIntervalUnit setting. For more information, see the App-V documentation on the Microsoft website at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	true
Default Value	
Accept Pipeline Input?	false

-GlobalRefreshIntervalUnit<>

Specifies the unit for the GlobalRefreshInterval setting. This can be set to either Hours (0) or Days (1). For more information, see the App-V documentation on the Microsoft website at http://technet.microsoft.com/en-us/library/jj687745.aspx

Required?	true
Default Value	
Accept Pipeline Input?	false

Examples

---------- EXAMPLE 1 ----------

```
Set-CtxAppVServerSetting -AppVPublishingServer http://AppV50Publishing:8082 -GlobalRefreshEnabled $true -GlobalRefreshOnLogon $true -GlobalRefreshInterval 2 -Globa
```

Test-CtxAppVServer

Sep 10, 2014

Tests the given URL for the presence of App-V Management and Publishing servers.

Syntax

```
Test-CtxAppVServer [-AppVManagementServer] <string> [<CommonParameters>]

Test-CtxAppVServer [-AppVPublishingServer] <string> [<CommonParameters>]
```

Detailed Description

Tests the given URL for the presence of App-V Management and Publishing servers.

Related topics

Parameters

-AppVManagementServer<String>

Machine name of the App-V Management server.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AppVPublishingServer<String>

Machine name of the App-V Publishing server.

Required?	false
Default Value	
Accept Pipeline Input?	false

Return Values

Microsoft.AppvAgent.AppvClientPackage

Examples

---------- EXAMPLE 1 ----------

```
Test-CtxAppVServer -AppVManagementServer “xmas-demo-appv”
```

Tests whether "xmas-demo-appv" is a Management server or not. The name does not need to be specified as a Fully Qualified Domain Name (FQDN).

---------- EXAMPLE 2 ----------

Test-CtxAppVServer -AppVPublishingServer “http://appvb2refserver.blrstrm.com:8082”
Tests whether “http://appvb2refserver.blrstrm.com:8082” is a Publishing server or not. Specify the full address, including FQDN and port number, of the Publishing server.

Citrix.Broker.Admin.V2

Sep 10, 2014

Overview

Name	Description
Broker AccessPolicy	Controls client-connection-based access to desktop groups.
Broker Applications	Describes how to publish and manage hosted applications.
Broker AssignmentPolicy	Controls the automatic, permanent assignment of machines to users.
Broker Concepts	Overview of the Citrix Broker.
Broker ConfigurationSlots	Overview of assigning a collection of related settings to a desktop group.
Broker ControllerDiscovery	Describes the way that machines providing published resources discover
Broker Desktops	Describes desktop concepts and usage.
Broker EntitlementPolicy	Controls end-user entitlement to desktop and application sessions provided
Broker ErrorHandling	Describes broker errors generated by cmdlets and how to access them.
Broker Filtering	Describes the common filtering options for XenDesktop cmdlets.
Broker Licensing	Overview of broker licensing configuration.
Broker Machines	Describes machine concepts and usage.
Broker Policies	Overview of the site policies that control users' access to desktop and
Broker PostInstallPreConfiguration	Describes how to configure the Citrix Broker Service port numbers, URL
Broker PowerManagement	Describes power management of machines used for desktops and applications.
Broker RemotePC	Overview of the Remote PC feature.

Cmdlets

Name	Description
Add-BrokerApplication	Adds applications to a desktop group.
Add-BrokerDesktopGroup	Associate Remote PC desktop groups with the specified Remote PC catalog.
Add-BrokerMachine	Adds one or more machines to a desktop group.
Add-BrokerMachineConfiguration	Adds a machine configuration to a desktop group.
Add-BrokerMachinesToDesktopGroup	Adds machines from a catalog to a desktop group.
Add-BrokerScope	Add the specified catalog/desktop group to the given scope(s).
Add-BrokerTag	Associate a tag with another object.
Add-BrokerUser	Creates an association between a user and another broker object
Disconnect-BrokerSession	Disconnect a session.
Export-BrokerDesktopPolicy	Gets the site wide Citrix Group Policy settings.
Get-BrokerAccessPolicyRule	Gets rules from the site's access policy.
Get-BrokerAdminFolder	Get the admin folders in this site.
Get-BrokerAppAssignmentPolicyRule	Gets application rules from the site's assignment policy.
Get-BrokerAppEntitlementPolicyRule	Gets application rules from the site's entitlement policy.
Get-BrokerApplication	Get the applications published on this site.
Get-BrokerApplicationInstance	Gets the running applications on the desktops.
Get-BrokerAssignmentPolicyRule	Gets desktop rules from the site's assignment policy.
Get-BrokerCatalog	Gets catalogs configured for this site.

Name	Description
Get-BrokerConfigurationSlot	Gets configuration slots configured for this site.
Get-BrokerConfiguredFTA	Gets any file type associations configured for an application.
Get-BrokerConnectionLog	Get entries from the site's session connection log.
Get-BrokerController	Gets Controllers running broker services in the site.
Get-BrokerDBConnection	Gets the database connection string for the specified data store used by the Broker Service.
Get-BrokerDBSchema	Gets SQL scripts to create or maintain the database schema for the Citrix Broker Service.
Get-BrokerDBVersionChangeScript	Gets an SQL service schema update script for the Citrix Broker Service.
Get-BrokerDelayedHostingPowerAction	Gets power actions that are executed after a delay.
Get-BrokerDesktop	Gets desktops configured for this site.
Get-BrokerDesktopGroup	Gets broker desktop groups configured for this site.
Get-BrokerDesktopUsage	Get usage history of desktop groups.
Get-BrokerEntitlementPolicyRule	Gets desktop rules from the site's entitlement policy.
Get-BrokerHostingPowerAction	Gets power actions queued for machines.
Get-BrokerHypervisorAlert	Gets hypervisor alerts recorded by the controller.
Get-BrokerHypervisorConnection	Gets hypervisor connections matching the specified criteria.
Get-BrokerIcon	Get stored icons.
Get-BrokerImportedFTA	Gets the imported file type associations.
Get-BrokerInstalledDbVersion	Gets a list of all available database schema versions for the Broker Service.
Get-BrokerLease	Gets stored leases.

Name	Description
Get-BrokerMachine	Gets machines belonging to this site.
Get-BrokerMachineCommand	Get the list of commands queued for delivery to a desktop.
Get-BrokerMachineConfiguration	Gets machine configurations defined for this site.
Get-BrokerMachineStartMenuShortcutIcon	Retrieves a Start Menu Shortcut icon from the specified machine.
Get-BrokerMachineStartMenuShortcuts	Retrieves the Start Menu Shortcuts from the specified machine.
Get-BrokerPowerTimeScheme	Gets power management time schemes for desktop groups.
Get-BrokerPrivateDesktop	Get private desktops configured for this site.
Get-BrokerRebootCycle	Gets one or more reboot cycles.
Get-BrokerRebootSchedule	Gets one or more reboot schedules.
Get-BrokerRemotePCAccount	Get RemotePCAccount entries configured for this site.
Get-BrokerResource	Gets resources that a user can broker connections to.
Get-BrokerScopedObject	Gets the details of the scoped objects for the Broker Service.
Get-BrokerServiceAddedCapability	Gets any added capabilities for the Broker Service on the controller.
Get-BrokerServiceInstance	Gets the service instance entries for the Broker Service.
Get-BrokerServiceStatus	Gets the current state of the Broker Service on the controller.
Get-BrokerSession	Gets a list of sessions.
Get-BrokerSessionLinger	Gets one or more session lingering settings.
Get-BrokerSessionPreLaunch	Gets one or more session pre-launch settings.

Name	Description
Get-BrokerSharedDesktop	Get shared desktops configured for this site.
Get-BrokerSite	Gets the current XenDesktop broker site.
Get-BrokerTag	Gets one or more tags.
Get-BrokerUnconfiguredMachine	Gets machines that have registered but are not yet configured in this site.
Get-BrokerUser	Gets broker users configured for this site.
Group-BrokerDesktop	Groups and counts desktops with the same value for a specified property.
Group-BrokerMachine	Groups and counts machines with the same value for a specified property.
Group-BrokerSession	Groups and counts sessions with the same value for a specified property.
Import-BrokerDesktopPolicy	Sets the site wide Citrix Group Policy settings for the site.
Move-BrokerAdminFolder	Moves a folder to another place in the hierarchy, optionally renaming it
Move-BrokerApplication	Move a published application from one admin folder to another
New-BrokerAccessPolicyRule	Creates a new rule in the site's access policy.
New-BrokerAdminFolder	Creates a new admin folder.
New-BrokerAppAssignmentPolicyRule	Creates a new application rule in the site's assignment policy.
New-BrokerAppEntitlementPolicyRule	Creates a new application rule in the site's entitlement policy.
New-BrokerApplication	Creates a new published application.
New-BrokerAssignmentPolicyRule	Creates a new desktop rule in the site's assignment policy.
New-BrokerCatalog	Adds a new catalog to the site.
New-BrokerConfigurationSlot	Creates a new configuration slot.

Name	Description
New-BrokerConfiguredFTA	Creates a file type association with a published application.
New-BrokerDelayedHostingPowerAction	Causes a power action to be queued after a delay.
New-BrokerDesktopGroup	Create a new desktop group for managing the brokering of groups of desktops.
New-BrokerEntitlementPolicyRule	Creates a new desktop rule in the site's entitlement policy.
New-BrokerHostingPowerAction	Creates a new action in the power action queue.
New-BrokerHypervisorConnection	Creates a new hypervisor connection.
New-BrokerIcon	Creates a new icon.
New-BrokerMachine	Adds a machine that can be used to run desktops and applications.
New-BrokerMachineCommand	Creates a new command to deliver to a desktop.
New-BrokerMachineConfiguration	Creates a new machine configuration associated with an existing configuration slot.
New-BrokerPowerTimeScheme	Creates a new power time scheme for a desktop group.
New-BrokerRebootSchedule	Creates a new reboot schedule for a desktop group.
New-BrokerRemotePCAccount	Create a new RemotePCAccount.
New-BrokerSessionLinger	Creates a new session linger setting for a desktop group.
New-BrokerSessionPreLaunch	Creates a new session pre-launch setting for a desktop group.
New-BrokerTag	Creates a new tag.
New-BrokerUser	Creates a new broker user object
Remove-BrokerAccessPolicyRule	Deletes a rule from the site's access policy.
Remove-BrokerAccessPolicyRuleMetadata	Deletes AccessPolicyRule Metadata from the AccessPolicyRule objects

Name	Description
Remove-BrokerAdminFolder	Removes an admin folder.
Remove-BrokerAdminFolderMetadata	Deletes AdminFolder Metadata from the AdminFolder objects
Remove-BrokerAppAssignmentPolicyRule	Deletes an application rule from the site's assignment policy.
Remove-BrokerAppEntitlementPolicyRule	Deletes an application rule from the site's entitlement policy.
Remove-BrokerApplication	Deletes one or more applications, or an association of an application.
Remove-BrokerApplicationInstanceMetadata	Deletes ApplicationInstance Metadata from the ApplicationInstance objects
Remove-BrokerApplicationMetadata	Deletes Application Metadata from the Application objects
Remove-BrokerAssignmentPolicyRule	Deletes a desktop rule from the site's assignment policy.
Remove-BrokerAssignmentPolicyRuleMetadata	Deletes AssignmentPolicyRule Metadata from the AssignmentPolicyRule objects
Remove-BrokerCatalog	Removes catalogs from the site.
Remove-BrokerCatalogMetadata	Deletes Catalog Metadata from the Catalog objects
Remove-BrokerConfigurationSlot	Removes a configuration slot.
Remove-BrokerConfigurationSlotMetadata	Deletes ConfigurationSlot Metadata from the ConfigurationSlot objects
Remove-BrokerConfiguredFTA	Deletes one or more configured file type associations.
Remove-BrokerControllerMetadata	Deletes Controller Metadata from the Controller objects
Remove-BrokerDelayedHostingPowerAction	Cancels one or more delayed power actions.
Remove-BrokerDesktopGroup	Remove desktop groups from the system or remove them from a Remote PC catalog.
Remove-BrokerDesktopGroupMetadata	Deletes DesktopGroup Metadata from the DesktopGroup objects

Name	Description
Remove-BrokerEntitlementPolicyRule	Deletes a desktop rule from the site's entitlement policy.
Remove-BrokerEntitlementPolicyRuleMetadata	Deletes EntitlementPolicyRule Metadata from the EntitlementPolicyRule objects
Remove-BrokerHostingPowerAction	Cancel one or more pending power actions.
Remove-BrokerHostingPowerActionMetadata	Deletes HostingPowerAction Metadata from the HostingPowerAction objects
Remove-BrokerHypervisorAlertMetadata	Deletes HypervisorAlert Metadata from the HypervisorAlert objects
Remove-BrokerHypervisorConnection	Removes a hypervisor connection from the system.
Remove-BrokerHypervisorConnectionMetadata	Deletes HypervisorConnection Metadata from the HypervisorConnection objects
Remove-BrokerIcon	Remove an icon.
Remove-BrokerIconMetadata	Deletes Icon Metadata from the Icon objects
Remove-BrokerImportedFTA	Deletes one or more imported file type associations.
Remove-BrokerLease	Remove the specified lease in the Database.
Remove-BrokerLeaseMetadata	Deletes Lease Metadata from the Lease objects
Remove-BrokerMachine	Removes one or more machines from its desktop group or catalog.
Remove-BrokerMachineCommand	Cancel a pending command queued for delivery to a desktop.
Remove-BrokerMachineCommandMetadata	Deletes MachineCommand Metadata from the MachineCommand objects
Remove-BrokerMachineConfiguration	Deletes a machine configuration from the site or removes the association from a desktop group.
Remove-BrokerMachineConfigurationMetadata	Deletes MachineConfiguration Metadata from the MachineConfiguration objects
Remove-BrokerMachineMetadata	Deletes Machine Metadata from the Machine objects
Remove-BrokerPowerTimeScheme	Deletes an existing power time scheme.

Name	Description
Remove-BrokerPowerTimeSchemeMetadata	Deletes PowerTimeScheme Metadata from the PowerTimeScheme objects
Remove-BrokerRebootCycleMetadata	Deletes RebootCycle Metadata from the RebootCycle objects
Remove-BrokerRebootSchedule	Removes the reboot schedule.
Remove-BrokerRemotePCAccount	Delete RemotePCAccounts from the system.
Remove-BrokerScope	Remove the specified catalog/desktop group from the given scope(s).
Remove-BrokerSessionLinger	Removes a session linger setting.
Remove-BrokerSessionMetadata	Deletes Session Metadata from the Session objects
Remove-BrokerSessionPreLaunch	Removes a session pre-launch setting.
Remove-BrokerSiteMetadata	Deletes Site Metadata from the Site objects
Remove-BrokerTag	Removes a tag from the system or clears a tag to object association.
Remove-BrokerTagMetadata	Deletes Tag Metadata from the Tag objects
Remove-BrokerUser	Remove broker user objects from another broker object
Rename-BrokerAccessPolicyRule	Renames a rule in the site's access policy.
Rename-BrokerAdminFolder	Renames a folder
Rename-BrokerAppAssignmentPolicyRule	Renames an application rule in the site's assignment policy.
Rename-BrokerAppEntitlementPolicyRule	Renames an application rule in the site's entitlement policy.
Rename-BrokerApplication	Renames an application.
Rename-BrokerAssignmentPolicyRule	Renames a desktop rule in the site's assignment policy.
Rename-BrokerCatalog	Renames a catalog.

Name	Description
Rename-BrokerDesktopGroup	Renames a desktop group.
Rename-BrokerEntitlementPolicyRule	Renames a desktop rule in the site's entitlement policy.
Rename-BrokerMachineConfiguration	Renames a machine configuration.
Rename-BrokerPowerTimeScheme	Changes the name of an existing power time scheme.
Rename-BrokerTag	Rename one or more tags.
Reset-BrokerLicensingConnection	Resets the broker's license server connection.
Reset-BrokerServiceGroupMembership	Reloads the access permissions and configuration service locations for the Broker Service.
Send-BrokerSessionMessage	Sends a message to a session.
Set-BrokerAccessPolicyRule	Modifies an existing rule in the site's access policy.
Set-BrokerAccessPolicyRuleMetadata	Creates/Updates metadata key-value pairs for AccessPolicyRule
Set-BrokerAdminFolderMetadata	Creates/Updates metadata key-value pairs for AdminFolder
Set-BrokerAppAssignmentPolicyRule	Modifies an existing application rule in the site's assignment policy.
Set-BrokerAppEntitlementPolicyRule	Modifies an existing application rule in the site's entitlement policy.
Set-BrokerApplication	Changes the settings of an application to the value specified in the command.
Set-BrokerApplicationInstanceMetadata	Creates/Updates metadata key-value pairs for ApplicationInstance
Set-BrokerApplicationMetadata	Creates/Updates metadata key-value pairs for Application
Set-BrokerAssignmentPolicyRule	Modifies an existing desktop rule in the site's assignment policy.
Set-BrokerAssignmentPolicyRuleMetadata	Creates/Updates metadata key-value pairs for AssignmentPolicyRule

Name	Description
Set-BrokerCatalog	Sets the properties of a catalog.
Set-BrokerCatalogMetadata	Creates/Updates metadata key-value pairs for Catalog
Set-BrokerConfigurationSlotMetadata	Creates/Updates metadata key-value pairs for ConfigurationSlot
Set-BrokerControllerMetadata	Creates/Updates metadata key-value pairs for Controller
Set-BrokerDBConnection	Configures a database connection for the Broker Service.
Set-BrokerDesktopGroup	Adjusts the settings of a broker desktop group.
Set-BrokerDesktopGroupMetadata	Creates/Updates metadata key-value pairs for DesktopGroup
Set-BrokerEntitlementPolicyRule	Modifies an existing desktop rule in the site's entitlement policy.
Set-BrokerEntitlementPolicyRuleMetadata	Creates/Updates metadata key-value pairs for EntitlementPolicyRule
Set-BrokerHostingPowerAction	Changes the priority of one or more pending power actions.
Set-BrokerHostingPowerActionMetadata	Creates/Updates metadata key-value pairs for HostingPowerAction
Set-BrokerHypervisorAlertMetadata	Creates/Updates metadata key-value pairs for HypervisorAlert
Set-BrokerHypervisorConnection	Sets the properties of a hypervisor connection.
Set-BrokerHypervisorConnectionMetadata	Creates/Updates metadata key-value pairs for HypervisorConnection
Set-BrokerIconMetadata	Creates/Updates metadata key-value pairs for Icon
Set-BrokerLeaseMetadata	Creates/Updates metadata key-value pairs for Lease
Set-BrokerMachine	Sets properties on a machine.
Set-BrokerMachineCatalog	Moves one or more machines into a different catalog.
Set-BrokerMachineCommandMetadata	Creates/Updates metadata key-value pairs for

Name	Description
Set-BrokerMachineConfiguration	Sets the properties of a machine configuration.
Set-BrokerMachineConfigurationMetadata	Creates/Updates metadata key-value pairs for MachineConfiguration
Set-BrokerMachineMaintenanceMode	Sets whether the specified machine(s) are in maintenance mode.
Set-BrokerMachineMetadata	Creates/Updates metadata key-value pairs for Machine
Set-BrokerPowerTimeScheme	Modifies an existing power time scheme.
Set-BrokerPowerTimeSchemeMetadata	Creates/Updates metadata key-value pairs for PowerTimeScheme
Set-BrokerPrivateDesktop	Change the settings of a private desktop.
Set-BrokerRebootCycleMetadata	Creates/Updates metadata key-value pairs for RebootCycle
Set-BrokerRebootSchedule	Updates the values of one or more desktop group reboot schedules.
Set-BrokerRemotePCAccount	Modify one or more RemotePCAccounts.
Set-BrokerSession	Sets properties of a session.
Set-BrokerSessionLinger	Updates the values of one or more desktop group session linger settings.
Set-BrokerSessionMetadata	Creates/Updates metadata key-value pairs for Session
Set-BrokerSessionPreLaunch	Updates the values of one or more desktop group session pre-launch settings.
Set-BrokerSharedDesktop	Change the settings of a shared desktop.
Set-BrokerSite	Changes the overall settings of the current XenDesktop broker site.
Set-BrokerSiteMetadata	Creates/Updates metadata key-value pairs for Site
Set-BrokerTagMetadata	Creates/Updates metadata key-value pairs for Tag

Name	Description
Start-BrokerCatalogPvdImagePrepare	Start the PVD Image prepare process in the Broker for the machines in the specified catalog(s).
Start-BrokerMachinePvdImagePrepare	Start the PVD Image prepare process in the Broker for the specified machine(s).
Start-BrokerNaturalRebootCycle	Reboots all machines from the specified catalog when they are not in use.
Start-BrokerRebootCycle	Creates and starts a reboot cycle for each desktop group that contains machines from the specified catalog.
Stop-BrokerRebootCycle	Cancels the specified reboot cycle.
Stop-BrokerSession	Stop or log off a session.
Test-BrokerAccessPolicyRuleNameAvailable	Determine whether the proposed AccessPolicyRule Name is available for use.
Test-BrokerAppAssignmentPolicyRuleNameAvailable	Determine whether the proposed AppAssignmentPolicyRule Name is available for use.
Test-BrokerAppEntitlementPolicyRuleNameAvailable	Determine whether the proposed AppEntitlementPolicyRule Name is available for use.
Test-BrokerApplicationNameAvailable	Determine whether the proposed Application Name is available for use.
Test-BrokerAssignmentPolicyRuleNameAvailable	Determine whether the proposed AssignmentPolicyRule Name is available for use.
Test-BrokerCatalogNameAvailable	Determine whether the proposed Catalog Name is available for use.
Test-BrokerDBConnection	Tests whether a database is suitable for use by the Citrix Broker Service.
Test-BrokerDesktopGroupNameAvailable	Determine whether the proposed DesktopGroup Name is available for use.
Test-BrokerEntitlementPolicyRuleNameAvailable	Determine whether the proposed EntitlementPolicyRule Name is available for use.
Test-BrokerLicenseServer	Tests whether or not a license server can be used by the broker.
Test-BrokerMachineNameAvailable	Determine whether the proposed Machine MachineName is available for use.

Name	Description
Test-BrokerPowerTimeSchemeNameAvailable	Determine whether the proposed PowerTimeScheme Name is available for use.
Test-BrokerRemotePCAccountNameAvailable	Determine whether the proposed RemotePCAccount OU is available for use.
Update-BrokerImportedFTA	Imports or updates all of the file type associations for the specified worker.
Update-BrokerLocalLeaseCache	Flushes the local lease cache.
Update-BrokerNameCache	Performs administrative operations on the user and machine name cache.

about_Broker_AccessPolicy

Sep 10, 2014

TOPIC

Citrix Broker SDK - Access Policy

SHORT DESCRIPTION

Controls client-connection-based access to desktop groups.

LONG DESCRIPTION

The site's access policy defines rules controlling a user's access to desktop groups. Access checks are based on details of the user's connection from their user device to the site. Think of the access policy informally as a connection-based firewall.

The access policy comprises a set of rules. Each rule:

- Relates to a single desktop group.
- Contains a set of connection filters and access right controls.

Multiple rules can apply to the same desktop group.

By default, users have no access to any desktop group within a site. A user gains access to a group when their connection's details match the connection filters of one or more rules in the access policy.

The access policy also grants control rights over desktop and application sessions. For example, it can specify which protocols are allowed for a connection from a given endpoint, and whether the user can restart their machine.

To use a resource published by a site, the user must have both access to the desktop group that contains it, and an entitlement to use the resource. Entitlements are typically granted by the site entitlement and assignment policies; see about_Broker_Policies for more information.

ACCESS POLICY RULES

A single access policy rule relates to a single specified desktop group and comprises a set of connection filters and access right grants as described below.

Each rule can be individually enabled or disabled. A disabled rule is ignored when the access policy is evaluated.

CONNECTION FILTERS OVERVIEW

The connection filters in an access policy rule comprise the following:

- Local/remote client (SmartAccess) filters
- Client IP address filters
- Client name filters
- User filters

All filters have an include and exclude form that can be individually enabled or disabled. For a rule to be considered when the access policy is evaluated, at least one connection include filter must be enabled. By default, all filters, both include and exclude, are disabled.

The detailed behavior of connection filters is covered later.

ACCESS RIGHT CONTROLS OVERVIEW

The access right controls in an access policy rule comprise the following:

- Allowed protocols
- Whether machine restart, or programmatic session logoff, is allowed

The detailed behavior of access right controls is covered later.

DETAILS OF CONNECTION FILTERS

To gain access to a desktop group the user's connection must match the filter criteria of at least one access policy rule for that group.

To match a rule, a connection must match all the rule's enabled include connection filters and must not match any of the rule's enabled exclude filters. That is, entries in exclude filters take priority.

Because all rules are evaluated independently, if an exclude filter match prevents a connection gaining access to a desktop group through one rule, the connection may still gain access to the same group through a different rule.

The filters are described in pairs below, but within a single rule a match against any exclude filter prevents a connection from gaining access through that rule irrespective of which include filters within the rule were also matched.

SMARTACCESS FILTERS

SmartAccess filters allow filtering based on whether the client is directly connected (for example over a local area network (LAN)) or through Access Gateway. For connections through Access Gateway further filtering can be performed based on the tags supplied from Access Gateway itself. The key properties of SmartAccess filters are:

- AllowedConnections (include filter: Filtered, NotViaAG, ViaAG)

  This property controls the behavior of the include filter. The default value is Filtered. The possible values are as follows:

  -- Filtered (default)

  The filter matches any user connection not through Access Gateway. In addition, the filter may match user connections through Access Gateway subject to the following: if the IncludedSmartAccessTags property is empty, any such connection matches. However, if the property is not empty at least one SmartAccess tag from the filter property must match a SmartAccess tag supplied with the user's

connection.

-- NotViaAG

The filter matches only user connections not through Access Gateway. The contents of the IncludedSmartAccessTags property are ignored.

-- ViaAG

The filter matches only user connections through Access Gateway. If the IncludedSmartAccessTags property is empty, any such connection matches. However, if the property is not empty at least one SmartAccess tag from the filter property must match a SmartAccess tag supplied with the user's connection.

The IncludedSmartAccessTags property referred to above forms part of the include filter and is used if AllowedConnections is set to Filtered or ViaAG. It comprises a simple list of Access Gateway tags that are matched against those provided in the user's connection details.

- ExcludedSmartAccessTags (exclude filter)

A simple list of Access Gateway tags that are matched against those provided in the user's connection details. If any tag in the list matches one supplied with the user's connection, the user's connection does not match the access policy rule containing the filter.

The exclude filter has no setting corresponding to the AllowedConnections property so its behavior is determined only by the ExcludedSmartAccessTags property.

SmartAccess filters are typically used to control local (through a LAN) and remote (through Access Gateway) access to a site. A common model is to define two access policy rules rules for a group, one for local access and one for remote. The remote rule might impose restrictions on the user device having appropriate antivirus software installed, and potentially exclude certain user groups who would be allowed access over the corporate LAN (see USER FILTERS below).

CLIENT IP FILTERS

Client IP filters allow filtering based on the IP address of the user's device. The key properties of client IP filters are:

- IncludedClientIPs (include filter)

A simple list of numeric IP address ranges that are matched against the user device. The filter matches if the device address falls within any of the ranges in the list.

- ExcludedClientIPs (exclude filter)

  A simple list of numeric IP address ranges that are matched against the user device. If any entry matches the device address, the user's connection does not match the access policy rule containing the filter.

An IP address range in these filters can be specified as a simple IP address or as a range using a conventional subnet mask.

CLIENT NAME FILTERS

Client name filters allow filtering based on the name of the user's device. The key properties of client name filters are:

- IncludedClientNames (include filter)

  A simple list of names that are matched against the user device. The filter matches if the device name matches any value in the list.

- ExcludedClientNames (exclude filter)

  A simple list of device names that are matched against the user device. If any entry matches the device name, the user's connection does not match the access policy rule containing the filter.

Note: The form of the device name presented to the site depends on the site configuration. For example, by default in these filters you cannot use the form of the name presented by Web Interface.

USER FILTERS

User filters allow filtering based on the identity of the user. The key properties of user filters are:

- AllowedUsers (include filter: Filtered, AnyAuthenticated, Any)

  This property controls the behavior of the include filter. The default value is Filtered. The possible values are as follows:

  -- Filtered (default)

  The filter matches if the user's logon token contains one or more users or user groups matching those specified in the IncludedUsers property. The IncludedUsers property is a simple list of users or user groups and is used only when the AllowedUsers property is set to Filtered.

  -- AnyAuthenticated

  The filter matches any authenticated Microsoft Windows user. The

contents of the IncludedUsers property are ignored.

-- Any

The filter matches any user. The contents of the IncludedUsers property are ignored. In the current implementation this value is handled in the same way as AnyAuthenticated.

- ExcludedUsers (exclude filter)

A simple list of users or user groups. If any entry matches one in the user's logon token, the user's connection does not match the access policy rule containing the filter.

The exclude filter has no setting corresponding to the AllowedUsers property so its behavior is determined only by the ExcludedUsers property.

DETAILS OF ACCESS RIGHT CONTROLS

The access right controls of an access policy rule determine rights that the user has over any desktop or application session that they obtain from the rule's desktop group.

The rights apply only if the user's connection matches the connection filters of a rule, and only if the user also has an entitlement to a desktop or application session from the associated desktop group.

The following properties define the access rights:

- AllowedProtocols

A simple list of communication protocols over which connections can be made to resources published by the desktop group. For example, use this to restrict protocols with high bandwidth requirements to connections originating from a LAN.

- AllowRestart

For single-session power-managed machines, allows the user to restart the machine (the machine is powered off using the capabilities of its hypervisor). For multi-session machines the user's session is simply logged off.

For a given connection, if multiple rules result in access being granted to a session from a desktop group, the user's rights are the combined rights of all the rules that matched for that group. The allowed protocol lists from all the rules are combined, and the user is granted restart rights if any one rule has AllowRestart set.

SEE ALSO

about_Broker_Policies

about_Broker_AssignmentPolicy

about_Broker_EntitlementPolicy

New-BrokerAccessPolicyRule

Get-BrokerAccessPolicyRule

Set-BrokerAccessPolicyRule

Rename-BrokerAccessPolicyRule

Remove-BrokerAccessPolicyRule

New-BrokerAssignmentPolicyRule

New-BrokerEntitlementPolicyRule

New-BrokerAppAssignmentPolicyRule

New-BrokerAppEntitlementPolicyRule

Add-BrokerUser

about_Broker_Applications

Sep 10, 2014

TOPIC

Citrix Broker SDK - Applications

SHORT DESCRIPTION

Describes how to publish and manage hosted applications.

LONG DESCRIPTION

Published applications allow your users to launch applications as if they were installed on their devices when in fact they are hosted remotely. The applications are normally launched in a seamless window, meaning that users see only the application window and not an additional desktop.

Published applications are hosted on either desktop operating systems or server operating systems. Applications are published to users and desktop groups. As such, conceptually they exist "on top" of desktop groups, which are themselves built on top of catalogs. See about_Broker_Concepts for more information on catalogs.

There are two types of applications:

- HostedOnDesktop - application runs on a remote machine and is displayed on the local client desktop.
- InstalledOnClient - application is installed and run on the local client machine and has its window overlaid on to a remote desktop.

HOSTING APPLICATIONS

There are three main ways of hosting an application: using a private single-session VDI desktop, a shared single-session VDI desktop, and on shared multi-session server operating systems.

An application hosted on a shared single-session VDI desktop, when launched, is hosted on a random machine within the desktop group. An application hosted on a private single-session VDI desktop ensures that when a user launches the application it is always hosted on the same machine. An application hosted on shared multi-session server operating systems ensures that when a user launches the application it is always hosted on one of the least loaded servers in the desktop group.

You control how the application is hosted based on the kind of desktop group that you choose. Shared desktop groups randomly select a machine, and these desktop groups can only be created from catalogs with a Random AllocationType. On the other hand, private desktop groups host the application on the same machine for that user every time, and these desktop group types can only be created from catalogs with a Permanent AllocationType.

USER ACCESS & ASSIGNMENT

Users are not assigned an application directly, but instead they are required to first have access to the desktop groups on which the applications are published through access policy rules.

With shared desktop groups, access to a published application also needs an application entitlement policy rule. An application entitlement policy rule defines the set of users who are allowed per-session access to desktops in a specified desktop group.

With private desktop groups, access to a published application also needs an application assignment policy rule. An application assignment policy rule defines the set of users who are allowed access to a single application session in a desktop group.

Users are assigned private machines in one of two ways: pre-assigned or assign-on-first-use. Pre-assigned means that individual user accounts have been specified for the machines within that desktop group. A single machine can only have a single user account (not a group account) assigned to it, and likewise a user can only be assigned a single machine within a desktop group.

Assign-on-first-use requires less configuration. Machines are assigned to users the first time they log on. Rather than allocating users directly to machines, instead users are assigned to the private desktop group, either through individual user accounts or through user group accounts. Then, when a user assigned to the desktop group logs on, a machine is automatically allocated to them.

USER VISIBILITY

Users can be further filtered by configuring the visibility filter on top of the application. This restricts the application to a subset of the users that were granted access by the access policy and entitlement/assignment policy rules on the desktop group.

MULTIPLE DESKTOP GROUPS

You can publish an application to multiple desktop groups, which have to be of the same kind. Generally, an application that is published only to private desktop groups is referred to as a "private application". An application that is only published to shared desktop groups is referred to as a "shared application".

LICENSING

Hosted applications need the appropriate licenses to exist on the license server to be functional.

NAMING

Applications have three names that identify them: the Name, BrowserName and the PublishedName. The Name is unique for each application, is not visible to the user, and is primarily used for administrative purpose. The BrowserName is unique across the entire site, and is primarily used internally. The PublishedName is not unique and is the name seen by end users who have access to this application.

When creating an application, you only need to specify the Name. If no BrowserName is specified one is automatically generated. If no PublishedName is specified by default it is the same as the Name.

The following special characters are not allowed in the Name, BrowserName or the PublishedName properties: \ / ; : # . * ? = < > | [ ] ( ) " '

In addition the ` character is not allowed in the Name property.

To change the PublishedName or BrowserName of an application you must use the Set-BrokerApplication cmdlet.

To change the Name of an application you must use the Rename-BrokerApplication cmdlet.

OPTIONAL

You can configure file-type associations for applications, so that if a user double-clicks a document icon on their device, a published application automatically starts. For more information, see the help for New-BrokerConfiguredFTA.

You can apply tags to applications as another convenient way to further organize (and search for) applications. For more information, see the help for New-BrokerTag.

CMDLETS

New-BrokerApplication

Creates an application for publishing after the needed desktop groups, access policy and entitlement/assignment policy rules have been created.

Add-BrokerApplication

Adds one or more applications to a desktop group.

Get-BrokerApplication

Gets one or more applications.

Remove-BrokerApplication

Deletes one or more applications or it can be used to delete just the association of an application to a desktop group.

Rename-BrokerApplication

Changes the Name of an application.

Set-BrokerApplication

Changes the settings of application objects, except their names.

EXAMPLES

SHARED APPLICATION (SingleSession)

You have created a catalog with a Random AllocationType and SingleSession SessionSupport. It contains two machines called worker1 and worker2, both in the ACME domain. You publish an application with shared hosting as follows:

```
C:\PS> Write-Host "Create a desktop group, and add machines to it"
C:\PS> $dg = New-BrokerDesktopGroup "Shared Application Group"
-DesktopKind Shared -DeliveryType AppsOnly -SessionSupport 'SingleSession'
C:\PS> $m1 = Get-BrokerMachine -MachineName "ACME\worker1"
C:\PS> $m2 = Get-BrokerMachine -MachineName "ACME\worker2"
C:\PS> Add-BrokerMachine $m1 -DesktopGroup $dg
C:\PS> Add-BrokerMachine $m2 -DesktopGroup $dg
C:\PS> Write-Host "Create access policy rule for desktop group"
C:\PS> New-BrokerAccessPolicyRule -Name "Shared Application Group - Allow Everyone Access"
-Enabled $true -DesktopGroupUid $dg.Uid -IncludedUserFilterEnabled $true
-AllowedProtocols @("HDX") -AllowedUsers AnyAuthenticated
C:\PS> Write-Host "Create application entitlement policy for desktop group"
C:\PS> New-BrokerAppEntitlementPolicyRule -Name "Shared Application Group - App Entitlement"
-IncludedUsers 'ACME\Domain Users' -DesktopGroupUid $dg.Uid -Enabled $true
C:\PS> Write-Host "Create an application"
C:\PS> New-BrokerApplication -Name "Notepad" -PublishedName "Notepad"
-CommandLineExecutable "notepad.exe" -DesktopGroup $dg.Uid
```

In turn, this set of commands: creates a shared single session desktop group for applications delivery; adds two machines (from a catalog with a Random AllocationType and SingleSession SessionSupport) to the desktop group; creates access policy and application entitlement policy rules; creates an application; specifies its name, the executable, and links the application to the desktop group that will host it.

SHARED APPLICATION (MultiSession)

You have created a catalog with a Random AllocationType and MultiSession SessionSupport. It contains one machine called worker1 in the ACME domain. You publish an application with shared hosting as follows:

```
C:\PS> Write-Host "Create a desktop group, and add machines to it"
C:\PS> $dg = New-BrokerDesktopGroup "Shared Application Group"
-DesktopKind Shared -DeliveryType AppsOnly -SessionSupport 'MultiSession'
C:\PS> $m1 = Get-BrokerMachine -MachineName "ACME\worker1"
C:\PS> Add-BrokerMachine $m1 -DesktopGroup $dg
C:\PS> Write-Host "Create access policy rule for desktop group"
C:\PS> New-BrokerAccessPolicyRule -Name "Shared Application Group - Allow Everyone Access"
-Enabled $true -DesktopGroupUid $dg.Uid -IncludedUserFilterEnabled $true
-AllowedProtocols @("HDX") -AllowedUsers AnyAuthenticated
C:\PS> Write-Host "Create application entitlement policy for desktop group"
C:\PS> New-BrokerAppEntitlementPolicyRule -Name "Shared Application Group - App Entitlement"
-IncludedUsers 'ACME\Domain Users' -DesktopGroupUid $dg.Uid -Enabled $true
C:\PS> Write-Host "Create an application"
```

```
C:\PS> New-BrokerApplication -Name "Notepad" -PublishedName "Notepad"
-CommandLineExecutable "notepad.exe" -DesktopGroup $dg.Uid
```

In turn, this set of commands: creates a shared multi session desktop group for applications delivery; adds one machine (from a catalog with a Random AllocationType and MultiSession SessionSupport) to the desktop group; creates access policy and application entitlement policy rules; creates an application; specifies its name, the executable, and links the application to the desktop group that will host it.

PRIVATE PRE-ASSIGNED APPLICATION

You have a catalog with a Permanent AllocationType and SingleSession SessionSupport. It contains two machines called worker1 and worker2, both in the ACME domain. You publish an application with private hosting using pre-assigned machines as follows:

```
C:\PS> Write-Host "Create a desktop group, and add machines to it"
C:\PS> $dg = New-BrokerDesktopGroup "Private App G1" -DesktopKind Private
-DeliveryType AppsOnly -SessionSupport 'SingleSession'
C:\PS> $m1 = Get-BrokerMachine -MachineName "ACME\worker1"
C:\PS> $m2 = Get-BrokerMachine -MachineName "ACME\worker2"
C:\PS> Add-BrokerMachine $m1 -DesktopGroup $dg
C:\PS> Add-BrokerMachine $m2 -DesktopGroup $dg
C:\PS> Write-Host "Setting access policy rule for desktop group"
C:\PS> New-BrokerAccessPolicyRule -Name "Private App G1 - Allow Everyone Access"
-Enabled $true -DesktopGroupUid $dg.Uid -IncludedUserFilterEnabled $true
-AllowedProtocols @("HDX") -AllowedUsers AnyAuthenticated
C:\PS> Write-Host "Pre-Assign users to the machines"
C:\PS> Add-BrokerUser "ACME\user1" -Machine $m1
C:\PS> Add-BrokerUser "ACME\user2" -Machine $m2
C:\PS> Write-Host "Create an application"
C:\PS> New-BrokerApplication -Name "Notepad" -PublishedName "Notepad"
-CommandLineExecutable "notepad.exe" -DesktopGroup $dg.Uid
```

In turn, this set of commands: creates a private desktop group for applications delivery; adds two machines (from a catalog with a Permanent AllocationType and SingleSession SessionSupport) to the desktop group; creates access policy; creates two user objects; pre-assigns a user to each machine; creates the application; assigns users to it; and links the application to the desktop group that will host it.

PRIVATE, ASSIGN-ON-FIRST-USE APPLICATION

You have a catalog created with a Permanent AllocationType and SingleSession SessionSupport. It contains two machines called worker1 and worker2, both in the ACME domain. You publish an application with private hosting using assign-on-first-use machines as follows:

```
C:\PS> Write-Host "Create a desktop group, and add machines to it"
```

```
C:\PS> $dg = New-BrokerDesktopGroup "Private App G2" -DesktopKind Private
-DeliveryType AppsOnly -SessionSupport 'SingleSession'
C:\PS> $m1 = Get-BrokerMachine -MachineName "ACME\worker1"
C:\PS> $m2 = Get-BrokerMachine -MachineName "ACME\worker2"
C:\PS> Add-BrokerMachine $m1 -DesktopGroup $dg
C:\PS> Add-BrokerMachine $m2 -DesktopGroup $dg
C:\PS> Write-Host "Setting access policy rule for desktop group"
C:\PS> New-BrokerAccessPolicyRule -Name "Private App G1 - Allow Everyone Access"
-Enabled $true -DesktopGroupUid $dg.Uid -IncludedUserFilterEnabled $true
-AllowedProtocols @("HDX") -AllowedUsers AnyAuthenticated
C:\PS> Write-Host "Create application assignment policy for desktop group"
C:\PS> New-BrokerAppAssignmentPolicyRule -Name "Private App G2 - App Assignment"
-IncludedUsers 'ACME\Domain Users' -DesktopGroupUid $dg.Uid -Enabled $true
C:\PS> Write-Host "Create an application"
C:\PS> New-BrokerApplication -Name "Notepad" -PublishedName "Notepad"
-CommandLineExecutable "notepad.exe" -DesktopGroup $dg.Uid
```

In turn, this set of commands: creates a private single session desktop group for applications delivery; adds two machines (from a catalog with a Permanent AllocationType and SingleSession SessionSupport) to the desktop group; creates access policy and application assignment policy rules; creates the application, and links the application to the desktop group that will host it.

SEE ALSO

about_Broker_Concepts

about_Broker_Desktops

New-BrokerApplication

Add-BrokerApplication

Remove-BrokerApplication

Rename-BrokerApplication

Set-BrokerApplication

New-BrokerAppAssignmentPolicyRule

Remove-BrokerAppAssignmentPolicyRule

Set-BrokerAppAssignmentPolicyRule

New-BrokerAppEntitlementPolicyRule

Remove-BrokerAppEntitlementPolicyRule

Set-BrokerAppEntitlementPolicyRule

about_Broker_AssignmentPolicy

Sep 10, 2014

TOPIC

Citrix Broker SDK - Assignment Policy

SHORT DESCRIPTION

Controls the automatic, permanent assignment of machines to users.

LONG DESCRIPTION

The site's assignment policy defines rules controlling automatic assignment of machines to users in a process referred to as Assign On First Use (AOFU).

In this assignment model, a desktop group is initially populated with machines that have no assignments, and users are granted entitlements to obtain a machine selected at random from the pool by self-service assignment. Once made, the assignment is permanent. The resulting assigned machines can be used to deliver either desktop or application sessions depending on the delivery type of the desktop group.

The assignment policy comprises a set of rules. The policy can be applied only to desktop groups of desktop kind Private.

For assignment of machines to deliver desktop sessions:

- Multiple rules can apply to the same desktop group.
- Each rule grants an entitlement to one or more machines.

For assignment of machines to deliver application sessions:

- Only a single rule can apply to a given desktop group.
- Each rule grants an entitlement to a single machine.
- Although only a single application assignment rule can be defined for a group, a user can still launch multiple applications from that group because the applications all run within the same session on the assigned machine.

Once a machine is assigned to a user by an assignment policy rule, the rule plays no further part in controlling access to that machine. The rule can be changed, or even removed, without impacting the user's access to the machine.

Rules for desktop and application machine assignments are distinct. Desktop assignments are managed through the BrokerAssignmentPolicyRule SDK object, and application rules through the BrokerAppAssignmentPolicyRule object.

Desktop machine assignment rules can be created only for desktop groups with delivery type DesktopsOnly, whereas an application machine assignment rule can be created only for delivery type AppsOnly.

Because desktop groups of assigned machines do not allow delivery type DesktopsAndApps, desktop machine assignment

and application machine assignment rules cannot exist for the same desktop group.

Assignment policy rules are also used to configure the RemotePC feature where their detailed usage differs. For more information on the RemotePC feature see "help about_Broker_RemotePC".

For an entitlement granted by the assignment policy to be available to a user, the site's access policy must also grant them access to the desktop group.

ASSIGNMENT POLICY RULES

Each assignment policy rule has the following key properties:

- The desktop group to which it applies (one rule only ever applies to one group).
- The users to which machines can be assigned by the rule.

Additionally for desktop assignment rules, the following properties exist:

- The published name of the entitlement (visible to the user).
- The number of machines (entitlements) to which the rule grants access.
- The properties that a newly assigned desktop acquires.

If multiple desktop assignment rules entitle a user to machines from the same desktop group, their total machine entitlement is the sum of those granted by all those rules. The properties of the desktop sessions obtained may differ depending on which of the entitlements the user selects to start a session.

Each rule can be individually enabled or disabled. A disabled rule is ignored when the assignment policy is evaluated.

USER FILTERS (FULL)

Each rule has two user filters, an include filter and an exclude filter:

- The include filter contains users and user groups that are granted entitlements to machines.
- The exclude filter contains users and user groups that are denied entitlements to machines.

If the include filter of a rule contains multiple instances of a user (either explicit or implicit), this does not alter the number of machine entitlements granted to them by the rule.

Entries in the exclude filter take priority, so if a user appears explicitly or implicitly in both filters, access is denied. Typically, you use this filter to exclude a user or group of users who would otherwise gain access because they are members of a user group specified in the include filter.

Because all rules are independently evaluated, the exclude filter can exclude only users who would otherwise gain an entitlement through the same rule's include filter. That is, if a user is in a rule's include filter but not its exclude filter, the rule

is guaranteed to grant that user access to a machine irrespective of whether the user appears in the exclude filter of other rules.

If a filter contains a user group that contains other users and groups, the filter implicitly includes all of those users and groups.

By default the exclude filter is disabled.

To maintain assignment policy rules that can be fully displayed and edited with Citrix Studio, use the simplified user filter model below and do not use the exclude filter.

USER FILTERS (SIMPLIFIED)

The included user filter described above also supports a simplified usage model where the filter itself is disabled. When this is done, any user who has access to the desktop group through the access policy is implicitly granted an entitlement to a machine through the entitlement policy rule without the need to list the user in the rule's include filter.

This is useful in cases where the access policy for the desktop group already explicitly specifies the users who should have access.

Even if the include filter is disabled, the exclude filter can still be used to deny the entitlement to users who would otherwise gain access through the access policy alone.

This simplified usage cannot be used for RemotePC desktop groups.

REMOTE PC USAGE

When a desktop group is configured as a RemotePC group, the usage of the assignment policy differs in the following ways:

- Only a single rule can apply to a given desktop group.
- The delivery type of the desktop group must be DesktopsOnly.
- The simplified user filter model cannot be used. Users or user groups must appear explicitly in the included user filter of the assignment policy rule.
- If the included user filter is disabled then RemotePC assignment for the group is also effectively disabled.

For more information on the RemotePC feature see "help about_Broker_RemotePC".

ADDITIONAL DESKTOP ASSIGNMENT RULE PROPERTIES

Desktop assignment rules specify the following additional properties:

- PublishedName
- Description
- IconUid
- ColorDepth
- SecureIcaRequired

The published name, description, and icon UID properties apply to the desktop entitlement itself and determine the way in which the entitlement is presented to the user in, for example, StoreFront.

The color depth and secure ICA properties apply to the desktop session that is obtained when the entitlement is used.

In all cases, these properties can be explicitly specified. However, a null value (the default) means that the corresponding property is taken from the desktop group to which the rule applies. This inheritance from groups is dynamic; if the property of the group changes, the property of the entitlement changes too.

For assignment rules these properties are copied to the newly assigned desktop when the granted entitlement is first used. If the properties on the rule are subsequently changed the properties on the user's assigned desktop do not change. The dynamic inheritance of desktop properties from the desktop group continues after the assignment has occurred if the original rule did not provide explicit property values.

CALCULATING OVERALL MACHINE ENTITLEMENTS

Assignment rules are modified only by the SDK; they are not modified when used by the system to make automatic assignments. The number of machine entitlements offered to the user is determined by the number of machines (within the desktop group) already assigned to them and by which rules those assignments were made.

For each desktop group, the number of desktop entitlements available to the user is determined as follows:

1. The total number of entitlements for the user to machines in the group,

   from all rules, is calculated.

2. The total number of assigned machines (from any source) that the user

   already has in the group is determined.

3. The outstanding entitlement value is derived as the difference of the

   above two numbers.

4. If the outstanding entitlement value is zero or fewer, no further

   entitlements are allowed.
   Otherwise, for each applicable rule, the number of entitlements is that defined by the rule itself, minus the number of desktops already assigned to the user by that rule, and capped by the outstanding entitlement value.

Desktop and application machine entitlements both follow the above rules. However, because only a single application assignment rule granting a single entitlement per group can exist, these rules are seldom a consideration for applications.

EXAMPLES

Simple case:
A user is entitled to a single machine in a group by a single assignment rule:

1. On first use, the user sees a single desktop entitlement. If the user selects this, a new desktop is assigned.
2. On subsequent uses, the user sees the assigned desktop only. No other entitlements are displayed.

Complex case:
A user is entitled to two machines, one from each of two different rules, A and B, both applying to the same desktop group. In addition, the user has a machine explicitly assigned to them by the administrator within that group:

1. On first use, the user sees the administrator-assigned desktop, a single entitlement to a desktop of type A, and a single entitlement to a desktop of type B. If either of the entitlements is selected, a desktop of the appropriate type, A or B, is assigned.
2. On subsequent uses, the user sees the administrator-assigned desktop and the desktop assigned by the selected entitlement. No further entitlements are displayed.

MACHINE ENTITLEMENT PRESENTATION

For desktop machine assignment rules, the user interface determines whether users can visually distinguish between an entitlement to a machine and an actual assigned desktop. This cannot be controlled by Broker SDK cmdlets.

Although the number of entitlements seen by users takes account of all of their currently assigned desktops, the dynamic state of the system can affect the user interaction. This means that entitlements are displayed even where the pool of machines is empty, or the remaining desktops are in maintenance mode or otherwise unavailable. If the user attempts to use an entitlement in these cases, they receive a no-available-desktop error.

For application machine entitlement rules, the entitlements themselves are not presented to the end user; only the applications available to the user are presented. The use of available assignments, or of already assigned machines, is managed automatically.

NOTES

If an assignment rule grants entitlements to a user group:

- The machine is assigned to the user who selects the entitlement, thus an assignment policy rule cannot be used to assign a machine to a user group. However, an administrator can assign a machine to a user group using the Add-BrokerUser cmdlet.
- The number of machine entitlements specified in a desktop assignment rule applies to each member of the user group. For example, if a rule grants a user group access to two machines, every user in the group is entitled to two desktops.

The total number of machine entitlements defined by the assignment policy for a given desktop group may exceed the number of machines present in the group. A user attempting to use an entitlement when the pool of machines is empty receives a no-desktop-available error. (See CALCULATING OVERALL MACHINE ENTITLEMENTS above).

A machine assigned to a user as a result of the assignment policy remains permanently assigned unless the machine assignment itself is removed by the administrator. Such assignments are permanent even if the assignment rule is deleted, when the machine is treated as administrator-assigned.

The assignment policy cannot be used to assign a machine to more than one user. This is only possible using the Add-BrokerUser cmdlet.

SEE ALSO

about_Broker_Policies

about_Broker_AccessPolicy

about_Broker_EntitlementPolicy

about_Broker_Applications

New-BrokerAssignmentPolicyRule

Get-BrokerAssignmentPolicyRule

Set-BrokerAssignmentPolicyRule

Rename-BrokerAssignmentPolicyRule

Remove-BrokerAssignmentPolicyRule

New-BrokerAppAssignmentPolicyRule

Get-BrokerAppAssignmentPolicyRule

Set-BrokerAppAssignmentPolicyRule

Rename-BrokerAppAssignmentPolicyRule

Remove-BrokerAppAssignmentPolicyRule

Add-BrokerUser

about_Broker_Concepts

Sep 10, 2014

TOPIC

Citrix Broker - Concepts

SHORT DESCRIPTION

Overview of the Citrix Broker.

LONG DESCRIPTION

The Citrix Broker is a Microsoft Windows service running on a delivery controller that responds to desktop/application launch requests from users through StoreFront by selecting a suitable machine, powering it up if necessary, and then returning the address of the selected machine to the user's endpoint system so that a session connection can be made. If required for resilience or scale, additional instances of the Broker may be installed to run on additional delivery controllers in the same delivery site.

In addition to handling launch requests, the Broker also has background responsibilities in the delivery site; these include: maintaining appropriate numbers of unused, powered-up machines to avoid unnecessary delays to users launching desktops/applications; maintaining periodic contact with powered-up machines; and monitoring the state of machines and user sessions.

The Citrix.Broker.Admin PowerShell snap-in provides the cmdlets needed to administer and monitor the behaviour of the Broker service, either on the local system (by default) or on another system (by use of the -AdminAddress command-line parameter).

The cmdlets in the broker SDK manage objects in the following broad functional areas:

PROVISIONING CONFIGURATION

The Broker must be informed of the machines which are at its disposal. In order to do this, machines are organized in catalogs, created with the New-BrokerCatalog cmdlet; machines are introduced into the system through the use of the New-BrokerMachine cmdlet.

Catalogs define the nature of the machines contained within them, such as the allocation type (that is, static or random), how the machines are actually provisioned (that is, by MCS, PVS or manually), whether they are physical or virtual machines, whether they are single-session or multi-session, etc.

Typically, machines configured from a provisioning standpoint are not associated with specific users (though they may need to be, for example if the machine's disk image was captured from a specific user's physical desktop using a P2V tool); this is normally done when configuring how resources are brokered to users, below.

It is also possible for a catalog to be configured to be populated automatically with end users' existing physical machines using the RemotePC feature. The about_Broker_RemotePC topic gives more detail.

Provisioning configuration involves the following SDK objects:

BrokerHypervisorConnection

BrokerCatalog
BrokerMachine
BrokerRemotePCAccount
BrokerUser

For more information, see:

Get-Help about_Broker_Machines
Get-Help about_Broker_RemotePC
Get-Help Get-BrokerHypervisorConnection
Get-Help Get-BrokerCatalog
Get-Help Get-BrokerMachine
Get-Help Get-BrokerUser

BROKERING CONFIGURATION

In order that resources (that is, desktops and applications) can be used in user sessions, the Broker must be configured to connect incoming user launch requests through StoreFront with the correct machine. This is achieved by adding machines to desktop groups. The grouping of machines in desktop groups need not necessarily match the grouping of the machines within the catalogs that were used for the configuration of provisioning. It is through the desktop group that the configuration of which users can use which machine resources is achieved.

Configuration of the mapping between resources and end users is achieved through a combination of machine assignment and entitlement rules. In addition, access to those resources must also be configured (for example, some resources could be configured only to be accessible to users when they are not connecting remotely through Access Gateway.) The about_Broker_Policies topic gives more detail of the rich configuration options available.

It is also possible for a desktop group to be configured to be populated automatically with end users' existing physical machines using the RemotePC feature. The about_Broker_RemotePC topic gives more detail.

When machines are virtual, the broker can be configured to minimize power usage by switching them off when they are not expected to be in use while still maintaining good response times for end-user launch requests. This is achieved through power policy for desktop groups. This allows separate configuration for peak compared to off-peak times of the week of the number of machines nominally to be powered up, the number of machines to be powered up and idling, in addition to those in use to be used as a "buffer" to ensure prompt servicing of user launch requests, and the behavior required for virtual machines when users disconnect from their sessions for extended periods of time.

It is also possible to issue explicit power commands to machines. The about_Broker_PowerManagement topic gives more detail.

Configuration of Brokering involves the following SDK objects:

BrokerDesktopGroup
BrokerPrivateDesktop
BrokerSharedDesktop
BrokerRemotePCAccount

BrokerPowerTimeScheme
BrokerUser
BrokerTag
BrokerAccessPolicyRule
BrokerAssignmentPolicyRule
BrokerEntitlementPolicyRule
BrokerApplication
BrokerApplicationInstance
BrokerAppAssignmentPolicyRule
BrokerAppEntitlementPolicyRule
BrokerConfiguredFTA
BrokerImportedFTA

For more information, see:

Get-Help about_Broker_Desktops
Get-Help about_Broker_Policies
Get-Help about_Broker_Applications
Get-Help about_Broker_RemotePC
Get-Help Get-BrokerPrivateDesktop
Get-Help Get-BrokerSharedDesktop
Get-Help Get-BrokerPowerTimeScheme
Get-Help Get-BrokerUser
Get-Help Get-BrokerTag
Get-Help Get-BrokerAccessPolicyRule
Get-Help Get-BrokerAssignmentPolicyRule
Get-Help Get-BrokerEntitlementPolicyRule

MONITORING AND ADMINISTRATION

After you have provisioned and configured machines for brokering, use the broker SDK to monitor and administer user sessions and other aspects of the delivery site.

Monitoring and administration involve the following SDK objects:

BrokerServiceStatus
BrokerHypervisorAlert
BrokerDesktop
BrokerDesktopUsage
BrokerHostingPowerAction
BrokerSession
BrokerSessionMessage

For more information, see:

Get-Help about_Broker_Desktops
Get-Help Get-BrokerServiceStatus
Get-Help Get-BrokerHypervisorAlert
Get-Help Get-BrokerDesktop
Get-Help Get-BrokerDesktopUsage
Get-Help Get-BrokerHostingPowerAction
Get-Help Get-BrokerSession
Get-Help Send-BrokerSessionMessage

SITE MANAGEMENT

The broker must be configured after installation; this is normally performed automatically by the Citrix Studio console. Configuration tasks include selecting the database (and obtaining the SQL scripting to initialize it), selecting the Citrix Configuration Service that holds the site configuration.

Note that some aspects of broker configuration (such as the port number on which the broker listens for SDK connections) cannot be configured with PowerShell cmdlets. These are configured through the use of the Broker Service executable. For more information, see about_Broker_PostInstallPreConfiguration.

A further important aspect of site management concerns the way in which machines providing resources identify the delivery controllers to which they belong. For more information, see about_Broker_ControllerDiscovery.

Managing XenDesktop sites involves the following SDK objects:

BrokerSite
BrokerController
BrokerDBConnection
BrokerDBSchema
BrokerDBVersionChangeScript
BrokerInstalledDbVersion
BrokerServiceInstance
BrokerServiceGroupMembership
BrokerNameCache

For more information, see:

Get-Help about_Broker_PostInstallPreConfiguration
Get-Help about_Broker_ControllerDiscovery
Get-Help Get-BrokerSite
Get-Help Get-BrokerController
Get-Help Get-BrokerDBConnection
Get-Help Get-BrokerDBSchema
Get-Help Get-BrokerDBVersionChangeScript
Get-Help Get-BrokerInstalledDbVersion
Get-Help Get-BrokerServiceInstance

```
Get-Help Reset-BrokerServiceGroupMembership
Get-Help Update-BrokerNameCache
```

about_Broker_ConfigurationSlots

Sep 10, 2014

TOPIC

Citrix Broker SDK - Configuration Slots and Machine Configurations

SHORT DESCRIPTION

Overview of assigning a collection of related settings to a desktop group.

LONG DESCRIPTION

Collections of related settings may be applied to individual desktop groups through the creation of configuration slots and machine configurations.

A configuration slot defines a collection of related settings that are to be associated with that slot. Each machine configuration is associated with a single configuration slot and provides specific values for settings of that slot.

The SettingsGroup property of the configuration slot determines the particular collection of related settings that are associated with that slot. These groups are defined by Citrix and are not modifiable by administrators. For example, there is a particular group of Profile management specific settings that may be associated with a configuration slot. Because of the close association between a configuration slot and its collection of related settings, the full set of configuration slots is created during the site creation.

Each machine configuration is associated with a single configuration slot. The machine configuration contains policy data that provides specific values for the settings associated with that configuration slot.

Every value set in a machine configuration's policy must belong to the configuration slot's settings group. Therefore the appropriate SDK snap-in must be used to create the policy data. For example, the Profile management snap-in must be used to create the policy data for a machine configuration associated with the Profile management configuration slot.

To have particular policy settings applied to the machines in a desktop group, a machine configuration is associated with that desktop group. A machine configuration may be associated with multiple desktop groups. A desktop group may be associated with multiple machine configurations.

When a machine configuration is associated with a desktop group, the configuration inherits the delegated administration restrictions of the desktop group. Thus, if a machine configuration is associated with multiple desktop groups, an administrator can only modify the policy data of the configuration if the administrator has permission to modify every one of those desktop groups.

For detailed information about defining and assigning machine configurations, see:

```
help New-BrokerMachineConfiguration
help Add-BrokerMachineConfiguration
```

SEE ALSO

New-BrokerConfigurationSlot

New-BrokerMachineConfiguration

Add-BrokerMachineConfiguration

Import-BrokerDesktopPolicy

about_Broker_ControllerDiscovery

Sep 10, 2014

TOPIC

Citrix Broker - Configuring Controller Discovery

SHORT DESCRIPTION

Describes the way that machines providing published resources discover delivery controllers.

LONG DESCRIPTION

In order for the broker to be able to connect users to desktops and applications, the machines from which they are published must register (that is, establish communication) with the broker on an appropriate delivery controller in the delivery site.

The default operation, whose configuration is described in this topic, is to use information from the registry. This is referred to as registry-based controller discovery. The registry information can be supplied when installing the delivery agent software on each machine or it can be supplied through group-policy.

If machines are provisioned using quick deploy, information about delivery controllers is stored in a special "identity disk" attached to the VM.

Finally, in some deployments, the use of an Organizational Unit (OU) in Active Directory (AD) may be preferred. This is referred to as AD-based controller discovery. In this case, you must configure the GUID of the OU in the machines' registries. Such configuration is not described in this topic.

To perform registry-based controller discovery, run the PowerShell script called Set-ADControllerDiscovery.ps1 that is installed on each controller in the folder:

```
$Env:ProgramFiles\Citrix\Broker\Service\Setup Scripts
```

For more information, run this script with the -help parameter.

about_Broker_Desktops

Sep 10, 2014

TOPIC

Citrix Broker SDK - Desktops

SHORT DESCRIPTION

Describes desktop concepts and usage.

LONG DESCRIPTION

A desktop is a machine that is able to run a Microsoft Windows desktop environment (with a shell, icons and taskbar) or individual applications (seamlessly integrated with the local desktop). The configuration of the desktop determines whether it can run only desktop environments, only applications, or both desktops and applications. Machines running workstation operating systems are able to run one session at a time (single-session), whereas machines running server operating systems have the ability to run multiple simultaneous sessions (multi-session).

A key aspect of desktops is how they are assigned (or allocated) to users. Two allocation types are supported:

- Random/Shared - A user is assigned a desktop at random from a pool of shared desktops. Multi-session desktops are able to run sessions to multiple users simultaneously, whereas single-session desktops can only run one session at a time, and are returned to the pool when the user logs off. Single-session shared desktops usually discard user data stored on them after the user logs off. Multi-session shared desktops, however, do not tend to discard user data after a log-off, as this is only possible when the desktop is rebooted by a reboot schedule.

- Permanent/Private - A private desktop is permanently assigned to a specific user and data stored on it is retained across logons and restarts. A private desktop can have users assigned explicitly or on first use.

DESKTOP GROUPS

Desktops are collected together in desktop groups, and these provide a flexible grouping mechanism that can be used to associate:

- Desktops running on a particular type of machine
- Desktops with particular software installed
- Desktops for a set of users
- Desktops accessed in a similar way
- Desktops configured in a particular way
- Any combination of the above

Each desktop group can only contain one type of desktop, determined by its AllocationType and SessionSupport properties.

When assigning shared desktops or assign-on-first-use (AOFU) desktops to users, the set of candidates comes from available desktops in a particular desktop group.

You configure power management policy for single-session desktop groups, including peak and off-peak settings, for each desktop group. See about_Broker_PowerManagement for details.

CREATION OF DESKTOPS

Desktop objects are created automatically when a machine is added to a desktop group. The type of desktop is determined by the AllocationType property of the desktop group.

In order for a machine to be added from a catalog, the machine must be compatible with the desktop group. For this to be true, the catalog's AllocationType must be compatible, and the SessionSupport property must match.

Note: Because the session support and functional level of the machine are determined by the software on the machine (operating system and Citrix VDA, respectively), the SessionSupport and MinimalFunctionalLevel of the catalog and desktop group may match, but not be compatible with the machine. In this case any attempt of registration by the machine will fail.

You can add machines explicitly using the Add-BrokerMachine cmdlet, or a number of free machines can be acquired from a catalog using the Add-BrokerMachinesToDesktopGroup cmdlet. A machine can only be associated with one desktop group at a time, and has a DesktopUid property that references the corresponding desktop object. You can also associate desktops to machines with their SID properties.

Desktop objects are deleted when the machine is removed from the desktop group (using the Remove-BrokerMachine cmdlet). Desktops are also deleted when the desktop group containing them is deleted (using the Remove-BrokerDesktopGroup cmdlet). A desktop cannot be removed from a catalog while it is in a desktop group.

SHARED (RANDOM) DESKTOPS

Shared desktops are published to users using entitlement policy rules. Each entitlement rule allows access to a single session on a desktop machine, selected at random from the available desktops in a desktop group (with a preference for desktops that are powered on). If there are no available desktops, launching the session fails. See about_Broker_EntitlementPolicy and about_Broker_PowerManagement for details.

PRIVATE (STATIC) DESKTOPS

You can assign private desktops to users explicitly or automatically, with the AOFU feature. It is also possible to assign private desktops to particular clients (through IP or client name).

You explicitly assign machines or desktops to users with the Add-BrokerUser cmdlet. Machines can be assigned to users before the machine has been added to the desktop group (desktop created), but otherwise the effect is the same.

With Add-BrokerUser you can assign a desktop to multiple users or user groups. If the desktop has single-session support then the desktop will be visible to multiple users, but only one user can log on to the desktop at any time.

Assignment policy rules allow you to use AOFU to assign desktops to users in a desktop group. When a user specified in an assignment policy rule launches a session, and if the user does not already have an assigned desktop, the broker selects an available desktop at random from the desktop group and permanently assigns it to that user. Once assigned in this way, the

desktop behaves as though the assignment was made explicitly by an administrator. See about_Broker_AssignmentPolicy for details.

It is possible to assign more than one desktop to a user. You can achieve this by explicit assignment, multiple assignment policy rules, or the MaxDesktops property of an assignment policy rule.

DESKTOP CONFIGURATION

When presented to the user, desktops are identified by:

- An icon (IconUid property)
- A name (PublishedName property)
- A description (Description property)

When starting the session, you can configure two connection settings:

- The color depth used at the start of the session (ColorDepth property)
- Whether SecureICA encryption is required (SecureIcaRequired property)

Each desktop group provides default values for these settings, but you can override them if the desktop has more specific settings (PrivateDesktop), or use an entitlement policy rule with more specific settings (SharedDesktop).

AOFU desktops can inherit these settings from the assignment policy rule when the assignment to the user takes place.

MAINTENANCE MODE

There are times when it is necessary to disable desktops. You can do this by setting the InMaintenanceMode property of a desktop to $true. This puts it into maintenance mode. The broker excludes single-session desktops in maintenance mode from brokering decisions and does not start new sessions on them. Existing sessions are unaffected. For multi-session desktops in maintenance mode, reconnections to existing sessions are allowed, but no new sessions are created on the machine.

Desktops in maintenance mode are also excluded from automatic power management, although explicit power actions are still performed.

Note that disabling desktop groups, entitlement policy rules, assignment policy rules, or applications are other ways of disabling aspects of brokering.

DESKTOP STATUS

Once desktops are created, you can query the configuration and state information for different kinds of desktop, or retrieve more information about desktops using the Get-BrokerMachine cmdlet. To get details of any sessions running on the desktops, use the Get-BrokerSession cmdlet.

You can also group desktops by a specific property, counting the number of desktops with each value using the Group-BrokerMachine cmdlet. This can provide useful summary statistics.

DESKTOP USAGE

Every hour the broker records how many desktops from each desktop group are in use, and the Get-BrokerDesktopUsage cmdlet returns this information. Analyze historical usage records to understand desktop usage patterns and help with the choice of idle pool and buffer settings.

DESKTOP CONDITIONS

CPU usage, ICA latency, and profile logon times of desktops are monitored. When one of these values exceeds a threshold (configured by policy), the condition is flagged in the DesktopConditions property of the desktop. When the value drops below the threshold again, the condition is cleared. Use Get-BrokerMachine or Group-BrokerMachines cmdlets to query this information.

SEE ALSO

about_Broker_Concepts

about_Broker_Applications

about_Broker_EntitlementPolicy

about_Broker_AssignmentPolicy

Add-BrokerMachine

Add-BrokerMachinesToDesktopGroup

Remove-BrokerMachine

Add-BrokerUser

Set-BrokerMachine

Set-BrokerPrivateDesktop

Get-BrokerMachine

Group-BrokerMachine

Get-BrokerDesktopUsage

about_Broker_EntitlementPolicy

Sep 10, 2014

TOPIC

Citrix Broker SDK - Desktop and Application Entitlement Policy

SHORT DESCRIPTION

Controls end-user entitlement to desktop and application sessions provided from a pool of shared machines.

LONG DESCRIPTION

The site's entitlement policy defines rules controlling users' entitlements to desktop and application sessions from pools of shared machines. Each pool is defined by a desktop group.

The entitlement policy comprises a set of rules. Each rule grants users a single entitlement to a desktop or application session in a specified desktop group. The policy can be applied only to groups of desktop kind Random. For desktop entitlements multiple rules can apply to the same group, however for application entitlements only a single rule can apply to a given group.

When the user starts a session by selecting an entitlement the behavior depends on the session-support property of the desktop group:

- For single-session groups the user is temporarily assigned a machine selected at random from the group to provide their session. When the session ends, the machine is returned to the pool of available machines.
- For multi-session groups the user session is provided by the machine that is least loaded within the group when the session is launched.

If multiple desktop entitlement rules for the same group contain the same user, the user can have as many desktop sessions from the group concurrently as they have entitlements.

Although only a single application entitlement rule can be defined for a group, a user can still launch multiple applications from that group because the applications all run within that entitlement's single session.

Rules for desktop and application session entitlements are distinct. Desktop entitlements are managed through the BrokerEntitlementPolicyRule SDK object, and application rules through the BrokerAppEntitlementPolicyRule object.

Desktop entitlement rules can be created only for desktop groups with delivery types DesktopsOnly or DesktopsAndApps, whereas an application entitlement rule can be created only for delivery types AppsOnly or DesktopsAndApps.

For desktop groups with delivery type DesktopsAndApps, typically one or more desktop session entitlement rules together with a single application session entitlement rule exist.

For an entitlement granted by the entitlement policy to be available to a user, the site's access policy must also grant them access to the desktop group.

ENTITLEMENT POLICY RULES

Each entitlement policy rule has the following key properties:

- The desktop group to which it applies (one rule only ever applies to one group)
- The users to whom the entitlement is granted

Additionally for desktop entitlement rules, the following properties exist:

- The published name of the entitlement (visible to the user)
- Any properties that a desktop session launched using the entitlement should use that differ from the defaults specified on the desktop group

If multiple desktop entitlements are available to a user from the same group the resultant desktop session properties may differ depending on which entitlement the user selects to start the session.

Each rule can be individually enabled or disabled. A disabled rule is ignored when the entitlement policy is evaluated.

USER FILTERS (FULL)

Each rule has two user filters, an include filter and an exclude filter:

- The include filter contains users and user groups that are granted an entitlement to a session
- The exclude filter contains users and user groups that are denied an entitlement to a session

If the include filter of a rule contains multiple instances of a user (either explicit or implicit), they get only one entitlement by that rule.

Entries in the exclude filter take priority, so if a user appears explicitly or implicitly in both filters, access is denied. Typically, you use this filter to exclude a user or group of users who would otherwise gain access because they are members of a user group specified in the include filter.

Because all rules are independently evaluated, the exclude filter can only exclude users who would otherwise gain an entitlement through the same rule's include filter. That is, if a user is in a rule's include filter but not its exclude filter, the rule is guaranteed to grant that user a session entitlement irrespective of whether the user appears in the exclude filter of other rules.

If a filter contains a user group that contains other users and groups, the filter implicitly includes all of those users and groups.

By default the exclude filter is disabled.

To maintain entitlement policy rules that can be fully displayed and edited with Citrix Studio, use the simplified user filter model below and do not use the exclude filter.

USER FILTERS (SIMPLIFIED)

The included user filter described above also supports a simplified usage model where the filter itself is disabled. When this is done, any user who has access to the desktop group through the access policy is implicitly granted an entitlement to a session through the entitlement policy rule without the need to list the user in the rule's include filter.

This is useful in cases where the access policy for the desktop group already explicitly specifies the users who should have access.

Even if the include filter is disabled, the exclude filter can still be used to deny the entitlement from users who would otherwise gain access through the access policy alone.

ADDITIONAL DESKTOP ENTITLEMENT RULE PROPERTIES

Desktop entitlement rules specify the following additional properties:

- PublishedName
- Description
- IconUid
- ColorDepth
- SecureIcaRequired

The published name, description, and icon UID properties apply to the desktop entitlement itself and determine the way in which the entitlement is presented to the user in, for example, StoreFront.

The color depth and secure ICA properties apply to the desktop session that is obtained when the entitlement is used.

In all cases, these properties can be explicitly specified. However, a null value (the default) means that the corresponding property is taken from the desktop group to which the rule applies. This inheritance from groups is dynamic; if the property of the group changes, the property of the entitlement changes too.

NOTES

If a rule grants an entitlement to a user group, the session entitlement applies to the individual user who selects the entitlement. However, this does not prevent a different user in the same user group from using the same entitlement concurrently. So, a rule that grants an entitlement to a user group containing multiple users allows each user concurrent access to a single session from the desktop group.

The total number of entitlements defined by the policy may exceed the number of machines available, or the maximum allowed sessions, from the desktop group. A user attempting to use an entitlement when no further resources are available receives a no-desktop-available error.

If a session launched through an entitlement is active when the entitlement rule is deleted, the session continues unaffected. However:

- When the user ends the session, they cannot start a new one if the deleted rule was their only entitlement to a session in that group
- If the user disconnects the session, they cannot reconnect to it

SEE ALSO

about_Broker_Policies

about_Broker_AccessPolicy

about_Broker_AssignmentPolicy

about_Broker_Applications

New-BrokerEntitlementPolicyRule

Get-BrokerEntitlementPolicyRule

Set-BrokerEntitlementPolicyRule

Rename-BrokerEntitlementPolicyRule

Remove-BrokerEntitlementPolicyRule

New-BrokerAppEntitlementPolicyRule

Get-BrokerAppEntitlementPolicyRule

Set-BrokerAppEntitlementPolicyRule

Rename-BrokerAppEntitlementPolicyRule

Remove-BrokerAppEntitlementPolicyRule

about_Broker_ErrorHandling

Sep 10, 2014

TOPIC

Citrix Broker SDK - Error Handling

SHORT DESCRIPTION

Describes broker errors generated by cmdlets and how to access them.

LONG DESCRIPTION

The broker SDK cmdlets report errors through the class SdkErrorRecord, which is a subclass of the standard Powershell error record class System.Management.Automation.ErrorRecord. SdkErrorRecord contains:

- A short string to describe the error status code. This is implemented as a public property named Status.
- A dictionary of key-value pairs containing additional data specific to the cmdlet. This is implemented as a public property named ErrorData of type Dictionary<string, string>.

The error status property always has a value. Populating the error data dictionary is optional. The number of entries within the dictionary, the content of the entries, and the exact format of the key and value data is specific to each cmdlet.

You can access an SdkErrorRecord object using the standard Powershell cmdlet ErrorVariable parameter. The type of object returned by ErrorVariable depends on whether the error is terminating or non-terminating.

NON-TERMINATING ERRORS

For non-terminating errors, each object in the returned ErrorVariable array is simply an instance of type SdkErrorRecord.

TERMINATING ERRORS

For terminating errors, the object returned by ErrorVariable is of type System.Management.Automation.CmdletInvocationException.

For non-terminating errors that are escalated as terminating errors (through the "ErrorAction stop" argument), the object returned by ErrorVariable is of type System.Management.Automation.ActionPreferenceStopException.

CmdletInvocationException and ActionPreferenceStopException are subclasses of the base class System.Management.Automation.RuntimeException, which exposes the SdkErrorRecord object through its ErrorData property.

Class SdkOperationException

SdkErrorRecord's Exception property holds an instance of custom exception class SdkOperationException, which also contains the error status code and data dictionary from SdkErrorRecord.

The SDK cmdlets generate errors in response to exceptions generated by the underlying system or by the cmdlet detecting

errors locally and instantiating appropriate exception types. Such exceptions, which represent the original cause of the terminating error, are specified in SdkOperationException's InnerException property.

For terminating errors, use Powershell scripts to trap SdkOperationException and access additional error information and the originating exception.

REVIEW OF POWERSHELL ERROR HANDLING BEHAVIOR

Powershell scripts can access error information using the following methods:

- Read error records from the $error arraylist.
- Get the cmdlet to return error records using the standard ErrorVariable cmdlet parameter.
- Use trap blocks to catch exceptions for terminating errors.

The type of the error record that Powershell puts in the $error arraylist and returns through the ErrorVariable cmdlet parameter depends on whether the error is terminating or non-terminating, and whether the "ErrorAction continue" or "ErrorAction stop" cmdlet parameters are specified (that turn terminating errors into non-terminating ones, and vice versa).

For the combinations of error types (terminating, non-terminating) and error actions (stop, continue), the following statements describe the relationship between:

- The type of object contained in the Powershell $error arraylist.
- The type of object returned by the ErrorVariable cmdlet parameter (assuming the script can continue after a terminating error).
- The type of the exception that is thrown (where applicable).

Non-terminating errors with ErrorAction=Continue, $error type=SdkErrorRecord, and ErrorVariable type=SdkErrorRecord do not throw an exception.

Terminating errors with ErrorAction=Stop, $error type=ErrorRecord, and ErrorVariable type=CmdletInvocationException throw an SdkOperationException exception.

Non-terminating errors with ErrorAction=Stop, $error type=ErrorRecord, and ErrorVariable type=ActionPreferenceOperationException do not throw an exception.

Terminating errors with ErrorAction=Continue, $error type=ErrorRecord, and ErrorVariable type= CmdletInvocationException throw an SdkOperationException exception.

ActionPreferenceOperationException and CmdletInvocationException are subclasses of System.Management.Automation.RuntimeException.

ACCESSING ERROR RECORD DATA

The Powershell code sample below demonstrates how to access error information programmatically with the ErrorVariable cmdlet parameter and a trap block.

```
# Trap exceptions generated from terminating errors trap [Exception] {
```



```
    write ""
    write "TRAP BLOCK : BEGIN"

    if($_.Exception.GetType().Name -eq "SdkOperationException")
    {
       $sdkOpEx = $_.Exception

       # show error status
       write $("SdkOperationException.Status = " + $sdkOpEx.Status)



   # show error data dictionary
       write $("SdkOperationException.ErrorData=")

       write $("SdkOperationException.InnerException = " + $sdkOpEx.InnerException)
       $_.Exception.ErrorData
    }

    continue #could also call break here to halt script execution
    write "TRAP BLOCK : END"

}

################################################################################ ## Run tests 1 to 4, below, in turn to examine terminating and ## non-terminating error behavior.
################################################################################

# # Test 1: Invoke cmdlet that generates a terminating error: # New-BrokerCatalog throws terminating error if a # catalog with the supplied name already exists. # #New-BrokerCatalog -Name "AlreadyExists" -AllocationType Random -ProvisioningType Manual -SessionSupport SingleSession -PersistUserChanges OnLocal -MachinesArePhysical $true -ErrorVariable ev

# # Test 2: Force script execution to continue after a terminating error. # #New-BrokerCatalog -Name "AlreadyExists" -AllocationType Random -ProvisioningType Manual -SessionSupport SingleSession -PersistUserChanges OnLocal -MachinesArePhysical $true -ErrorVariable ev -ErrorAction continue

# # Test 3: Invoke cmdlet that generates a non-terminating error: # Get-BrokerCatalog generates a non-terminating error if a catalog # with the specified name doesn't exist. # #Get-BrokerCatalog -Name "IDontExist" -ErrorVariable ev

# # Test 4 Force script execution to halt after a non-terminating error. # #Get-BrokerCatalog -Name "IDontExist" -ErrorVariable ev -ErrorAction "stop"

write "" write "GET ERROR INFORAMTION: BEGIN"

$sdkErrRecord = $null

if ($ev[0].GetType().Name -eq "SdkErrorRecord") {
```



```
        $sdkErrRecord = $ev[0]

}

elseif($ev[0].GetType().BaseType.FullName -eq "System.Management.Automation.RuntimeException") {


        $sdkErrRecord = $ev[0].ErrorRecord

} else {


      write ("UNKNOWN ERROR VARIABLE TYPE:")
      $ev[0].GetType().Name

}

if($sdkErrRecord -ne $null) {


        write ("Have sdkErrRecord:")
        write ("  Type Name = " + $sdkErrRecord.GetType().FullName)
        write ("  Status = " + $sdkErrRecord.Status)
        write ("  Exception type = " + $sdkErrRecord.Exception.GetType().FullName)
        write ("  ErrorData = ")
        $sdkErrRecord.ErrorData
        write ("  FullyQualifiedErrorId = " + $sdkErrRecord.FullyQualifiedErrorId)

} write "GET ERROR INFORAMTION: END"
```

about_Broker_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more
are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```

retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

A120901
B220000
...

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

about_Broker_Licensing

Sep 10, 2014

TOPIC

Citrix Broker - Licensing

SHORT DESCRIPTION

Overview of broker licensing configuration.

LONG DESCRIPTION

As part of the licensing setup for a site, the types of product licenses used by the broker when creating connections to virtual desktops or applications can be configured using the Central Configuration Service SDK.

The following licensing related properties can be specified using the Set-ConfigSite cmdlet:

- LicensingModel - Sets the licensing model to use. Values can be 'Concurrent' or 'UserDevice'.
- ProductCode - Specifies which product license is supported by the site. Values can be "MPS" for XenApp licenses or "XDT" for XenDesktop licenses.
- ProductEdition - Sets the licensing edition to use.

A license matching the specified model, product code, and edition must be available within the site's license server in order for the broker to grant licenses.

These properties are part of the site object returned by the Get-ConfigSite cmdlet.

CONCURRENT LICENSE MODEL

A concurrent license is tied to a XenDesktop session. When a user launches a session, a license is checked out to that session. When a user logs off from a session, the license is checked back in again, making it available for another session.

USER DEVICE LICENSE MODEL

With user device licensing, the license server automatically assigns licenses to users or devices based on usage:

- User licensing allows users to access their desktops and applications from multiple devices.
- Device licensing allows multiple users to access their desktops and applications from a single device.

When users or devices connect to an application or desktop, they consume a license for a 90-day license assignment period. The assignment period begins when a connection is made, is renewed to the full 90 days during the life of the connection, and expires (allowing reassignment) 90 days after the last connection terminates. A license assignment can be manually

ended before the 90-day period elapses using the udadmin command line installed on the license server.

LICENSING STATE

The broker site contains the following properties related to licensing state:

- LicensingGracePeriodActive - Reports if the broker is in licensing grace period.
- LicensingOutOfBoxGracePeriodActive - Reports if the broker is in out-of-box grace period.
- LicensingGraceHoursLeft - The number of grace hours remaining, if the broker is in grace period, else it is null.
- LicensedSessionsActive - The number of active, licensed sessions.
- LicenseGraceSessionsRemaining - The number of grace sessions available, if the broker is in licensing grace period, else it is null.

These properties are part of the site object returned by the Get-BrokerSite cmdlet.

LICENSE SERVER TEST

The broker SDK cmdlet Test-BrokerLicenseServer checks whether or not a given server can be used as a license server by the broker.

RESETTING LICENSE SERVER CONNECTION

The broker SDK cmdlet Reset-BrokerLicensingConnection resets the broker's connection to the license server.

LICENSE BURN-IN DATE

The version of the product that is supported within the site is denoted by a licensing burn-in date. This date can be accessed through the LicensingBurnInDate field of the site object returned by the Get-ConfigSite cmdlet.

SEE ALSO

about_Broker_Site

Test-BrokerLicenseServer

Reset-BrokerLicensingConnection

Get-BrokerController

Set-ConfigSite

Get-ConfigSite

Get-BrokerSite

about_Broker_Machines

Sep 10, 2014

TOPIC

Citrix Broker SDK - Machine Object

SHORT DESCRIPTION

Describes machine concepts and usage.

LONG DESCRIPTION

A machine represents a physical or virtual machine that can be used to provide a user with one or more desktops, applications or both. When a machine is created, you must assign it to a catalog, which defines how the machine is allocated to a user (static or random), the session support it provides (single-session or multi-session), how the machine's disk images are created and managed (PVS, MCS or manually) and the expected functional level. If the machine is virtual but not provisioned by MCS, you must also assign it to a hypervisor connection, which represents the hypervisor (or pool of linked hypervisors) that runs the virtual machine.

Creating a machine object is the first step in the broker SDK towards configuring a physical or virtual machine to provide desktops and/or applications to users. A machine must be added to a desktop group before it is able to be used(see about_Broker_Desktops). To add machines to a desktop group, the Add-BrokerMachine or Add-BrokerMachinesToDesktopGroup cmdlets can be used. This creates a desktop object corresponding to the machine.

CATALOGS

When a machine is created, you must assign it to a catalog. The catalog defines the behavior of the machine within a site as well as the expected functionality and properties of the machine:

- Allocation type: The catalog determines how the machines are allocated to the user. Allocation can be static or random. Static allocation is where the machine is permanently assigned to a specific user. Data stored is retained across logons and restarts.

  The other type of allocation is random, where a random machine is assigned to a user from a pool when a session is requested. The machine returns to the pool when the user logs off.

- How the machine is created: The catalog collects together machines that are created in the same way: either with PVS, MCS or manually.

- Physical or Virtual: A machine that is virtual can have its power state controlled and monitored by the system. Virtual machines must be associated with a hypervisor connection, either directly or, in the case of MCS provisioned machines, indirectly through the provisioning scheme. Single session virtual machines can be managed using power policy to automatically be turned on or off as needed. Machines marked as physical are not monitored or controlled as to their power state.

- How the users settings are stored: The catalog also determines how the users settings are stored, either on a Citrix Personal vDisk, on the machine's local drive, or if the user settings are discarded.

- RemotePC: If the catalog is set up as a remote PC catalog, machines are added automatically upon registration based on the site configuration. In order for a catalog to be specified as a RemotePC catalog, the session support must be single session and the catalog must be set up for physical machines.

- Functional level: The functional level of a machine is determined by the version of the Citrix VDA software it is running. Some features are not supported in machines with lower functional levels. Catalogs can supply a minimal functional level, meaning any machines in the catalog with a lower functional level will be unable to register with the site.

- Session support: This can either be single-session or multi-session. Single-session machines can have an active session with up to one user at any time, whereas multi-session machines have the capability to have active sessions with multiple users simultaneously. The session support of a machine is determined by the variant of the VDA software component installed on the machine (either with single-session support or multi-session support). The multi-session VDA software may only be installed on server operating systems. The catalog session support must match the session support of the software installed on the machine for the machine to successfully register with the site.

MACHINE STATUS

After machines are created, you can query the configuration and state information using the Get-BrokerMachine cmdlet. The information the cmdlet can provide includes, but is not limited to, the following:

- Personal vDisk interactions and lifecycle: The current state of the personal vDisk can be obtained, as well as the configuration options of how the user data is persisted.

- Session properties: The properties of the current session for single-session machines can be obtained, such as ClientName and ClientAddress. To access session information on multi-session machines, the Get-BrokerSession cmdlet can be used.

- Application status: If the machine is configured to run applications, information can be found about the published applications running on the machine.

- Connection information: Information about the time and user of the last

connection to the machine can be found, as well as information about the last deregistration.

For an exhaustive list of the properties of a machine that can be queried, see the Get-BrokerMachine cmdlet.

MACHINE CONFIGURATION

Machine settings can be changed and configured once the machine object has been created, as long as the changes are compatible with the catalog the machine is in. For example, more users can be assigned to the machine than were initially assigned when creating the machine object, this is done with the Add-BrokerUser cmdlet.

For a full list of the machine configuration options available, see the Set-BrokerMachine command.

MAINTENANCE MODE

There are times when it is necessary to disable machines. This can be achieved by setting the InMaintenanceMode property to $true. This puts the machine into maintenance mode. With single-session machines, this means that the broker excludes the machine from brokering decisions and does not start new sessions on them. Existing sessions are unaffected. For multi-session desktops in maintenance mode, reconnections to existing sessions are allowed, but no new sessions are created on the machine.

Machines in maintenance mode are also excluded from automatic power management, although explicit power actions are still performed.

SEE ALSO

about_Broker_PowerManagement

about_Broker_Desktops

New-BrokerMachine

Add-BrokerMachine

Add-BrokerMachinesToDesktopGroup

Remove-BrokerMachine

Get-BrokerMachine

Set-BrokerMachine

about_Broker_Policies

Sep 10, 2014

TOPIC

Citrix Broker SDK - Access, Entitlement, and Assignment Policies

SHORT DESCRIPTION

Overview of the site policies that control users' access to desktop and application sessions.

LONG DESCRIPTION

For an end user to access a desktop or application resource within a site, they must have both an entitlement to use the resource, and have access to the desktop group that contains the resource.

Entitlements to use resources can be granted by one of the following means:

- The site entitlement policy grants entitlements to launch a shared desktop or application session from a pool of shared machines.
- The site assignment policy grants entitlements for "self service" permanent assignment of machines to users for running desktop or application sessions, and is referred to as "Assign On First Use" (AOFU)
- Machines can be permanently assigned ("pre-assigned") to users by the administrator to run either desktop or application sessions.
- Machines can be configured to allow automatic permanent assignment to their normal user (using the RemotePC feature).

A user must also be granted access to the desktop group that contains the resource. These access rights are controlled by the site's access policy.

The access policy controls access using details of the user's device such as whether it's connected over a local area network (LAN) or connected through Access Gateway, the user device's name, IP address or subnet, and the requested connection protocol. The user's identity can also feed into the access check allowing, for example, certain users access to resources only when locally connected to the site, but others full remote access.

Access and entitlements can be combined to allow rich and fine-grained control over which users have access to site resource from any given user device or location.

Each site has a single access policy, entitlement policy, and assignment policy. Each policy comprises a set of rules. Policies are defined by adding, removing, or changing rules.

Each site policy can also be viewed as a set of distinct policies each relating to a single desktop group. In general a group has one or more policy rules that relate to it, however each rule relates to only a single group. Thus the rules that grant entitlement and access rights to a desktop group define the policy for that group and that group only; changing this policy has no impact on the entitlement and access rights for any other other group in the site.

For detailed information about defining policy rules, see:

```
help New-BrokerAccessPolicyRule
help New-BrokerEntitlementPolicyRule
help New-BrokerAssignmentPolicyRule
help New-BrokerAppEntitlementPolicyRule
help New-BrokerAppAssignmentPolicyRule
```

The mapping of policies to the resources that they make available within a site is described briefly below. For specific information on configuring each category of resource, consult the more detailed help topics listed.

SHARED DESKTOP AND APPLICATION SESSIONS

To grant access to a group of shared machines, use the access and entitlement policies:

- The access policy grants access to the desktop group containing the machines to be shared.
- The entitlement policy grants an entitlement to use one or more machines in the group to specified users or groups of users.

Groups of shared machines can be used to deliver full desktop or seamless application sessions, or both.

For more detailed information about configuring shared machines, see:

```
help about_Broker_AccessPolicy
help about_Broker_EntitlementPolicy
```

PRE-ASSIGNED PRIVATE MACHINES

To grant access to private machines, use the access policy and a machine assignment:

- The access policy grants access to the desktop group containing the machines.
- The assignment links the desktop to a specified user. You can assign a machine to just one user, multiple users or user groups. However, for single-session machines, only one user can access the machine at a time.

Private machines can be used to deliver full desktop or seamless application sessions (but not both).

For more detailed information about configuring private machines, see:

```
help about_Broker_AccessPolicy
help Add-BrokerUser
```

ASSIGN-ON-FIRST-USE (AOFU) MACHINES

To grant access to a desktop group containing assignable machines, use the access policy and the assignment policy:

- The access policy grants access to the desktop group containing the pool of machines.
- The assignment policy grants users a self-service entitlement to pick one or more machines from the pool.

AOFU machines can be used to deliver full desktop or seamless application sessions (but not both from the same desktop group).

For more detailed information about configuring AOFU desktops, see:

```
help about_Broker_AccessPolicy
help about_Broker_AssignmentPolicy
```

REMOTE PC MACHINES

The RemotePC feature allows existing physical machines to be assigned automatically to their normal user thus allowing them remote access to their own machine but without the need for the administrator to individually configure access to each machine.

For more detailed information about configuring the Remote PC feature, see:

```
help about_Broker_RemotePC
```

SEE ALSO

about_Broker_AccessPolicy

about_Broker_EntitlementPolicy

about_Broker_AssignmentPolicy

about_Broker_RemotePC

New-BrokerAccessPolicyRule

New-BrokerEntitlementPolicyRule

New-BrokerAssignmentPolicyRule

New-BrokerAppEntitlementPolicyRule

New-BrokerAppAssignmentPolicyRule

Add-BrokerUser

about_Broker_PostInstallPreConfiguration

Sep 10, 2014

TOPIC

Citrix Broker SDK - Post-Installation Configuration

SHORT DESCRIPTION

Describes how to configure the Citrix Broker Service port numbers, URL reservations, and Windows Firewall exclusions.

LONG DESCRIPTION

The XenDesktop installer configures the Citrix Broker Service with information specified during the installation. To change that configuration, use the BrokerService.exe command-line tool on each controller you want to change.

The default installation location of BrokerService.exe is:

```
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe
```

BrokerService.exe supports the following optional command-line parameters:

-SdkPort <port> (default 80)

Configures the port on which the broker listens for requests from SDK cmdlets. If you change this default value, specify the new value in the AdminAddress parameter on broker cmdlets. For example, if you changed the port to 8080, specify it as follows:

```
Get-BrokerSite -AdminAddress localhost:8080
```

-VdaPort <port> (default 80)

Configures the port on which the broker listens for registration requests from broker machines.

-WiPort <port> (default 80)

Configures the port on which the broker listens for XML requests from StoreFront/Web Interface.

-WiSslPort <port> (default 443)

Configures the port on which the broker listens for SSL (Secure Socket Layer) XML requests from StoreFront/Web Interface.

-ConfigureFirewall

Configures Windows Firewall exclusions for the specified ports.

-Show

Shows the current configuration settings.

-Uninstall

Removes configuration settings, including Windows Firewall exclusions and URL reservations.

-LogFile <fileName>

Configures the file location for logging to a text file. The directory containing the log file must grant write access to the NetworkService account.

-Upgrade

Performs configurations required after an upgrade.

-Quiet

Suppresses console output for status messages.

-? or -Help

Shows usage information for the command.

about_Broker_PowerManagement

Sep 10, 2014

TOPIC

Citrix Broker SDK - Machine Power Management

SHORT DESCRIPTION

Describes power management of machines used for desktops and applications.

LONG DESCRIPTION

The Citrix Broker Service is in day-to-day control of the power state of the configured desktop and application machines. The Broker Service can control several hypervisors, each hypervisor connection being handled by its own site service, so all Broker Service communication to the hypervisor is through one of the controllers in the site.

HYPERVISOR CONNECTIONS

Each hypervisor, or pool of linked hypervisors, is described and configured through the XdHyp pseudo-drive and associated Hyp PowerShell commands (cmdlets) which are provided by the host service snap-in. When you have first created the hypervisor connection using the host service cmdlets, you can create a broker equivalent object that references the Hyp instance using a GUID value. Use the broker's HypervisorConnection object to nominate a preferred controller for direct communication with the hypervisor on behalf of all other controllers for day-to-day power actions and status requests.

POWER ACTIONS AND THROTTLING

The site, through the Broker Service, can control the power state of the machines used by the site for desktops and applications. Power state changes can have a number of causes:

- Power policy rules, such as requests to shut down or suspend machines when user sessions on those machines end or are disconnected
- If allowed, user-driven desktop restarts
- Session launch requests requiring machines to be started
- Pool size management, which controls the number of running machines
- Direct administrator request using the SDK or Citrix Studio
- Reboot schedules and cycles
- Performing personal vDisk inventory activities
- Cleaning machines back to the golden master image state after they have been used

The power state changes of machines hosting desktops and applications are controlled using a queuing mechanism. Actions to change the power state are assigned a priority and are sent to the hypervisor according to a throttling mechanism. This avoids overloading the hypervisor.

The queuing and throttling mechanisms take place on a per-hypervisor-connection basis; each hypervisor connection's queue is dealt with independently. You can view the contents of the queues using the Get-BrokerHostingPowerAction cmdlet. This includes recently completed, in-progress, and pending actions (that is, those due to be sent to the hypervisor

based on the throttling settings).

Each power action object comprises:

- The machine to be acted on (Name, DNS Name, Hosting Name)
- The action to be performed (TurnOn, TurnOff, Shutdown, Reset, Restart, Suspend, or Resume)
- The action's priority (Base, the original priority, and Actual, the current priority)
- The action's state (Pending, Started, Completed, Failed, Canceled, Deleted, or Lost)
- Time stamps of the action's lifecycle points (when it was created, started, or completed)
- Any reason the action failed

The throttling of power actions is controlled by three metadata values on the Hyp hypervisor connection object when accessed through the XdHyp pseudo-drive. The four values throttle power actions according to:

- The maximum absolute number of in-progress power actions
- The maximum number of in-progress power actions expressed as a percentage of the total number of machines controlled by the hypervisor connection
- The maximum number of new power actions sent to the hypervisor per minute
- The maximum number of in-progress PvD inventory activities expressed as a percentage of the total number of machines controlled by the hypervisor connection

You add power actions to the queue using the SDK's New-BrokerHostingPowerAction cmdlet. You cancel power actions in the queue using the Remove-BrokerHostingPowerAction cmdlet. You boost or reduce their priority using the Set-BrokerHostingPowerAction cmdlet.

You can also schedule power actions to be executed in the future, using the New-BrokerDelayedHostingPowerAction command. Only Shutdown and Suspend actions can be scheduled in this way. You can view these delayed power actions using Get-BrokerDelayedHostingPowerAction and cancel them with Remove-BrokerDelayedHostingPowerAction. When a delayed power action is ready to be executed it is deleted, and a corresponding normal power action is placed in the queue described above.

POWER POLICY

Policy rules associated with a desktop group allow you to change power states at configurable times after session state changes, typically a set number of minutes after session disconnection or session logout.

Note that these policy rules are defined directly as properties of the desktop group.

These policy actions allow the following operations to be specified:

- A power action to be performed at a defined period after a session is disconnected
- A power action to be performed at a defined extended period after a session is disconnected
- A power action to be performed at a defined period after a session is logged off

The two disconnect policy actions are designed to allow multi-stage policies such as initially suspending a machine shortly after a session disconnect occurs, and then later powering-off the machine if the session has not been reconnected.

At the set time after the session state change, the required action is added to the power action queue, and this is then throttled and processed as normal.

POOL SIZE MANAGEMENT

You can manage flexibly the number of machines running desktops and applications using the pool size. For any given hour of the day and day of the week, this is an absolute number of machines or the percentage of the total number of machines in the desktop group. The pool size specifies the total number of machines that are always running, regardless of whether they are in use or idle. (Note: The number of machines does not depend on their idle status, but this does affect the buffer size value, which is also used to manage pool sizes.)

To start or shut down desktop machines to achieve the desired pool size, the system places power actions in the queue. Standard throttling queue management sends these to the hypervisors. A single desktop group (and its pool) can span multiple hypervisors, so actions to start and shut down machines can be added to multiple queues.

POWER TIME SCHEMES

Each single-session desktop group can be associated with one or more power time schemes, each scheme covering a number of days of the week. The time schemes specify, for each hour of the day, whether that hour is peak or off-peak. They also specify the number of running unassigned machines maintained by the broker.

You can configure other settings, such as buffer size and any power policy rules differently for peak and off-peak hours. You can define the number of running machines, idle or in use, either as an absolute value or as a percentage of the desktop group size. Machines running desktops and applications are started (or shut down when not in use) to match the required pool size.

Each power time scheme comprises:

- The name of the scheme
- The pattern of days of the week covered by the scheme
- The set of hours considered peak and off peak
- The set of pool size values (one for each hour of the day)

The hours of the day used by time schemes are the hours in the time zone for the desktop group the scheme is associated with. You cannot associate one desktop group with multiple time schemes covering the same day of the week.

BUFFER SIZE

In addition to the pool size, you can optionally configure two buffer sizes for each desktop group, one for peak hours and one for off-peak hours. The buffer size defines the minimum number of idle unassigned machines maintained by the broker and is specified as a percentage of the total machines in the group. These are running machines that are not used by any user session. The buffer size on its own never causes machines to shut down. It causes them to start up so a minimum number of idle machine is always available. The buffer size in conjunction with the pool size can cause machines running desktops or applications to be shut down.

POWER MANAGEMENT OF ASSIGNED MACHINES

Automatic power management for private desktop groups provides the ability to power on all assigned machines at the transition to a peak period and respectively power off all machines at the transition to an off-peak period.

If a machine is shut down during peak hours it will not be automatically powered on again, unless the AutomaticPowerOnForAssignedDuringPeak property on the desktop group is also enabled.

Note that all power management facilities apply only to single session machines.

REBOOT SCHEDULES

Reboot schedules are commonly used after image updates or to perform regular reboots of all machines in a desktop group or catalog to clear down problems resulting from a corrupt state or hung/faulty applications.

Reboot schedules allow distributing the reboot operation of all machines over a provided duration. Individual machine reboots are scheduled in a way that attempts to maintain maximum availability of machines in the group as the reboots occur, and avoid boot storms that overload the underlying infrastructure.

Reboot schedules are the only form of automatic power management that can shut down a machine while users are logged on; however the administrator can provide a warning message to be displayed to end users at a specified period prior to the shutdown taking effect.

REBOOT CYCLES

Reboot cycles describe the dynamic execution of desktop group or catalog reboot operations. Reboot cycles can be created due to reboot schedules, or by on-demand reboot operations requested via the SDK.

RebootCycle objects encapsulate the details of the associated reboot operation and can be queried to show the current status.

STATUS

You can view the status of the hypervisor connection on the broker hypervisor connection object. You can obtain any hypervisor alerts using the Get-BrokerHypervisorAlert cmdlet. You can check the power state of machines running desktops or applications using the relevant Machine or Desktop objects.

SEE ALSO

about_Broker_Concepts

about_Broker_Machines

about_HypHostSnapin

New-BrokerHypervisorConnection

Get-BrokerHypervisorConnection

Set-BrokerHypervisorConnection

Remove-BrokerHypervisorConnection

New-BrokerHostingPowerAction

Get-BrokerHostingPowerAction

Set-BrokerHostingPowerAction

Remove-BrokerHostingPowerAction

New-BrokerDelayedHostingPowerAction

Get-BrokerDelayedHostingPowerAction

Remove-BrokerDelayedHostingPowerAction

New-BrokerPowerTimeScheme

Get-BrokerPowerTimeScheme

Set-BrokerPowerTimeScheme

Rename-BrokerPowerTimeScheme

Remove-BrokerPowerTimeScheme

Get-BrokerRebootCycle

Set-BrokerRebootCycleMetadata

Start-BrokerRebootCycle

Stop-BrokerRebootCycle

Get-BrokerRebootSchedule

Set-BrokerRebootSchedule

New-BrokerRebootSchedule

Remove-BrokerRebootSchedule

New-BrokerDesktopGroup

Get-BrokerDesktopGroup

Set-BrokerDesktopGroup

Add-HypMetadata

Remove-HypMetadata

about_Broker_RemotePC

Sep 10, 2014

TOPIC

Citrix Broker SDK - RemotePC

SHORT DESCRIPTION

Overview of the Remote PC feature.

LONG DESCRIPTION

Remote PC allows automatic publishing of a user's physical desktop within a XenDesktop site, so that it can be accessed remotely. The configuration of Remote PC within the Citrix Broker service specifies the rules and relationships that allow the machine to successfully register with a controller in the site, and be made available for the user to start remote sessions.

When Remote PC is configured, there are two steps required for publishing a machine as a Remote PC desktop.

First a VDA must be installed on the machine and it must be configured such that it registers with a controller in a site.

Second, a user must log on to the machine. When the Citrix Broker service detects an active console session for a user, it assigns the user to the machine and publishes it in a Remote PC desktop group.

Remote PC configuration consists of defining relationships between:

- Machines and catalogs
- Catalogs and desktop groups
- Desktop groups and assignment policy rules
- Assignment policy rules and users

The Citrix Broker service automates the assignment of Remote PC machines to users in two stages. The first stage automatically imports matching unconfigured machines into the site:

- Suitable machines are automatically added to a Remote PC catalog.
- The machines are temporarily configured to be in one of the Remote PC desktop groups associated with the catalog.

When a suitable user logs on to the console of the machine, the second stage of the automatic configuration is performed:

- The machine is configured to be in the desktop group that is appropriate for the user.
- The machine is assigned to the user that has logged on.
- The machine desktop is made available to the user remotely, configured

to appear as the machine hostname.

Catalogs and desktop groups can be marked as participating in RemotePC automation with the 'IsRemotePC' property, but this property can only be set to true if various other properties of the catalog or desktop group are appropriate. Catalogs must be single-sessioned and contain physical machines. Desktop Groups must be single session, configured to deliver private assigned machines, delivering desktop sessions only.

Catalogs and desktop groups can have the 'IsRemotePC' property cleared to remove them from the RemotePC automation, but only when all RemotePC associations relating to them through RemotePCAccounts and catalog/group relationships have first been removed.

MACHINES AND CATALOGS

Mappings are defined between machines and Remote PC catalogs through the RemotePCAccount cmdlets.

The machine to catalog mappings support the automated addition of machines to catalogs.

PROPERTIES

RemotePCAccounts expose sets of included and excluded machine name filters specified in DOMAIN\MACHINE format. A MachinesIncluded or MachinesExcluded entry can include asterisk wildcards to generalize matches.

Each RemotePCAccount can specify the Distinguished Name (DN) of an AD container in addition to the machine name filters, in the RemotePCAccount Organisational Unit (OU) property, and this limits the machines that the account objects act on to those that reside at or below that container in the AD domain hierarchy. An AllowSubfolderMatches setting on the RemotePCAccount indicates whether the computer must exist directly within the container to trigger a match, or whether it can be in a child below the defined container in the AD hierarchy.

Note that the AD container component is optional and a special value of 'any' can be supplied in the OU field to permit the RemotePCAccount to automatically match regardless of the AD machine object location in the AD domain hierarchy. A match is still subject to machine name filtering.

The last component of the RemotePCAccount is the CatalogUid. This indicates which catalog the Remote PC automation should move the machine into when a match is found.

CONSTRAINTS

The IsRemotePC setting must be enabled on catalogs before they can be specified in a RemotePCAccount.

There can be any number of RemotePCAccounts configured in the site as long as each specifies a unique OU. There can be only one RemotePCAccount with the 'any' OU.

AUTOMATION

When a machine matching the criteria set up in a RemotePCAccount instance registers with one of the brokers in the site, it is automatically added to the catalog defined by the RemotePCAccount. This can take up to 30 seconds to happen after the machine registers.

When the machine registration occurs, the machine details can match more than one RemotePCAccount instance, but the machine can only be placed into one catalog, so one RemotePCAccount instance is chosen from the list that best matches the machine. This choice is made according to the length in nodes of the DN of the AD container specification associated

with the RemotePCAccount, so more specific child OUs override specifications for their parent OUs if both are present. The RemotePCAccount for the 'any' OU is always last and used only if no other instances match.

A Windows eventlog message is generated when an automated catalog assignment is performed.

NOTES

The AD distinguished name for the container is checked when the RemotePCAccount is created, but if the container is subsequently moved or deleted, the site does not automatically accommodate this, and the RemotePCAccount must be changed or removed manually.

Related Cmdlets

o New-BrokerRemotePCAccount

o Get-BrokerRemotePCAccount

o Set-BrokerRemotePCAccount

o Remove-BrokerRemotePCAccount

o New-BrokerCatalog [-IsRemotePC <Boolean>]

o Set-BrokerCatalog [-IsRemotePC <Boolean>]

CATALOGS AND DESKTOP GROUPS

A Remote PC catalog may be associated with one or more Remote PC desktop groups. The catalog to desktop group associations support automated publishing of machines to users.

USAGE

An association is formed via:

```
Add-BrokerDesktopGroup -RemotePCCatalog <Catalog> [-Priority <Int32>]
```

An association is broken via:

```
Remove-BrokerDesktopGroup -RemotePCCatalog <Catalog>
```

To find associated desktop groups:

```
Get-BrokerDesktopGroup -RemotePCCatalogUid <Int32>
```

AUTOMATION

When a machine in a Remote PC catalog is not already assigned to a user, Remote PC automation temporarily places the machine in one of the desktop groups associated with the catalog. The temporary placing of the machine in a group will be

adjusted as needed when the machine assignment to a user is first made.

The desktop group chosen as the temporary home for a machine is according to the priority value supplied when making the association between the group and the catalog. The group with the highest priority (lowest numerical priority value) is chosen.

A Windows eventlog message is generated when an automated machine assignment is performed.

PRIORITY

Each desktop group to catalog association has a priority value that can be specified when the association is made or defaults to lower than the lowest existing association priority (highest numerical value) or zero if no other association exists yet. The lower the priority numerical value, the higher the priority level. The priority value for the association is used to choose the temporary desktop group to place a new RemotePC machine in when it first registers. It is also used to decide which group to finally place the machine in when the user that the machine is being assigned to is appropriate for more than one of the associated desktop groups, usually because the desktop groups are using AD security groups for the user associations with the desktop groups.

The priority values for each association between a desktop group and a catalog are automatically maintained as unique for each catalog, and priorities can be adjusted up or down accordingly by the system. The last association created without a specified priority is always arranged to have the least priority (the highest numerical priority value).

NOTES

The temporary placement of the machines in a desktop group is not re-evaluated if settings change after the automatic placement.

RELATED CMDLETS

o Add-BrokerDesktopGroup -RemotePCCatalog <Catalog>

o Remove-BrokerDesktopGroup [-RemotePCCatalog <Catalog>]

o Get-BrokerDesktopGroup [-RemotePCCatalogUid <Int32>]

o New-BrokerCatalog [-IsRemotePC <Boolean>]

o Set-BrokerCatalog [-IsRemotePC <Boolean>]

o New-BrokerDesktopGroup [-IsRemotePC <Boolean>]

o Set-BrokerDesktopGroup [-IsRemotePC <Boolean>]

DESKTOP GROUPS, ASSIGNMENT POLICY RULES, AND USERS

Assignment policy rules are used to define sets of users allowed to be assigned to machines by Remote PC automation, and to determine which desktop group the machine is placed in when the user assignment is made.

AUTOMATION

A machine is automatically assigned to a user when the Citrix Broker service sees that the user has logged on to a RemotePC machine, and the user is amongst those configured in the desktop group assignment policy rule. If this is the first assignment of a user to a machine, all the assignment policy rules for all groups associated with the machine are checked, and the machine can be moved to a different, more appropriate desktop group if needed.

A Windows eventlog message is generated when an automated assignment of a machine to a user is made.

MULTIPLE ASSIGNMENTS

By default, multiple automatic assignments of users to the same machine can be established if multiple users log on to the RemotePC machine, but this can be disabled if desired using a registry setting (see CTX137805).

NOTES

User to machine assignments can still be made and removed manually through the Powershell SDK for machines in Remote PC catalogs and desktop groups.

The automatic placement of a machine in an appropriate desktop group happens when the first automatic assignment of a user to the machine is made, and this placement will not be automatically updated if the configuration subsequently changes.

Only a single assignment policy rule is allowed for each RemotePC desktop group.

RELATED CMDLETS

o New-BrokerUser

o New-BrokerAssignmentPolicyRule

o Set-BrokerAssignmentPolicyRule

EXAMPLE

```
The following example creates a simple configuration that allows any user
and machine in the current AD domain to participate in RemotePC.

# Create a Remote PC catalog
$catalog = New-BrokerCatalog -IsRemotePC $true
                    -SessionSupport SingleSession
                    -MachinesArePhysical $true
                    -AllocationType Static
                    -PersistUserChanges OnLocal
                    -ProvisioningType Manual
                    -Name RemotePCCatalog

# Create a Remote PC desktop group
$dg = New-BrokerDesktopGroup -IsRemotePC $true
                    -SessionSupport SingleSession
                    -DeliveryType DesktopsOnly
                    -DesktopKind Private
                    -Name RemotePCDesktopGroup

# Create an assignment policy rule for that desktop group allowing any
# domain user to match.
New-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid
```

```
                    -IncludedUsers 'domain users'
                    -Name RemotePCAPR

# Create a RemotePCAccount matching any unconfigured machine, causing the
# machines to be added to the catalog by Remote PC automation.
New-BrokerRemotePCAccount -OU 'any'
                  -CatalogUid $catalog.Uid

# Associate the desktop group and catalog to permit domain users to be
# automatically assigned to machines in that catalog
Add-BrokerDesktopGroup $dg -RemotePCCatalog $catalog

#Create an access policy rule, allowing access to the users to the
#Remote PC desktop group.
New-BrokerAccessPolicyRule -IncludedUsers 'domain users'
                    -DesktopGroupUid $dg.Uid
                    -IncludedUserFilterEnabled $true
                    -Name RemotePCAccessPolicyRule
```

Add-BrokerApplication

Sep 10, 2014

Adds applications to a desktop group.

Syntax

```
Add-BrokerApplication [-InputObject] <Application[]> [-DesktopGroup <DesktopGroup>] [-Priority <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Add-BrokerApplication [-Name] <String> [-DesktopGroup <DesktopGroup>] [-Priority <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Add-BrokerApplication cmdlet is used to associate one or more applications with an existing desktop group.

There are two parameter sets for this cmdlet, allowing you to specify the application either by its BrowserName or by an array of object references. Uids can also be substituted for the object references.

See about_Broker_Desktops and about_Broker_Applications for more information.

Related topics

New-BrokerApplication

Add-BrokerApplication

Add-BrokerTag

Remove-BrokerApplication

Rename-BrokerApplication

Move-BrokerApplication

Set-BrokerApplication

Parameters

-InputObject<Application[]>

Specifies the application to associate. Its Uid can also be substituted for the object reference.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the application to be associated with the desktop group.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroup<DesktopGroup>

Specifies which desktop group this application should be associated with. Note that applications can only be associated with desktop groups of the AppsOnly or DesktopsAndApps delivery type.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-Priority<Int32>

Specifies the priority of the mapping between the application and desktop group where lower numbers imply higher priority with zero being highest.

If one association has a higher priority than the other, machines from that group will be selected for launching sessions until all machines are at maximum load, in maintenance mode, unregistered, or unavailable for any other reason. Only when all machines from the higher-priority group are unavailable will new connections be routed to the next lowest priority group.

If multiple associations have equal priority, load balancing does not occur among the desktop groups in these associations. Instead, the broker chooses one of these groups as the preferred group and machines from this group will be selected for launching sessions until all machines are at maximum load, in maintenance mode, unregistered, or unavailable for any other reason. Only when all machines from the preferred group are unavailable will new connections be routed to another one of these groups, which the broker chooses as next-most preferred.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Application, or as appropriate by property name You can pipe the application to be added to Add-BrokerApplication. You can also pipe some of the other parameters by name.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Add-BrokerApplication -BrowserName "Notepad" -DesktopGroup "Private DesktopGroup"
Adds the application with a BrowserName of "Notepad" to the desktop group called "Private DesktopGroup".

Add-BrokerDesktopGroup

Sep 10, 2014

Associate Remote PC desktop groups with the specified Remote PC catalog.

Syntax

Add-BrokerDesktopGroup [-InputObject] <DesktopGroup[]> [-RemotePCCatalog <Catalog>] [-Priority <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-BrokerDesktopGroup [-Name] <String> [-RemotePCCatalog <Catalog>] [-Priority <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

This cmdlet forms relationships between Remote PC desktop groups and catalogs.

The Remote PC relationships are used by Remote PC automation to determine which desktop groups a machine in a particular Remote PC catalog can be published to. The assignment policy rules belonging to those desktop groups also determines the set of users that are allowed to be assigned to machines from the catalog.

Related topics

Remove-BrokerDesktopGroup

Add-BrokerCatalog

Remove-BrokerCatalog

Parameters

-InputObject<DesktopGroup[]>

Specifies one or more Remote PC desktop groups to add to a Remote PC catalog.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the Remote PC desktop groups to add to a Remote PC catalog based on their name properties.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-RemotePCCatalog<Catalog>

The Remote PC catalog which the desktop groups are to be added to. Specified by name, Uid or instance.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-Priority<Int32>

Desktop group to catalog associations carry a priority number, where numerically lower values indicate a higher priority.

The priority relative to other associations determines which desktop group Remote PC automation will move a qualifying unconfigured machine into when it registers. Priority also determines which desktop group a machine will be published to when a user is assigned to the machine by Remote PC automation.

If a value is not supplied, then the desktop group association is automatically assigned a lower priority than any existing associations.

If a priority value is specified that conflicts with an existing association's priority value, then the new association is inserted with that value and existing associations are renumbered upwards to accommodate it.

Required?	false
Default Value	See description
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.DesktopGroup The set of Remote PC desktop groups to be added to the catalog can be piped into this cmdlet.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerDesktopGroup -IsRemotePC $true | Add-BrokerDesktopGroup -RemotePCCatalog 42
Add all Remote PC desktop groups to Remote PC catalog 42.

---------- EXAMPLE 2 ----------

C:\PS> Add-BrokerDesktopGroup -Name *MyGroup* -RemotePCCatalog RPCCat
Add desktop groups with names containing MyGroup to Remote PC catalog with name "RPCCat".

Add-BrokerMachine

Sep 10, 2014

Adds one or more machines to a desktop group.

Syntax

Add-BrokerMachine [-InputObject] <Machine[]> [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-BrokerMachine [-MachineName] <String> [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Add-BrokerMachine cmdlet adds specified machines to a desktop group. There are three forms:

o Use the -InputObject parameter to add a single machine instance or array of instances to the group.

o Use the -MachineName parameter to add a single, named machine to the group.

o Use pipelining to pipe machines instances to the command.

The desktop group to which the machines are added can be specified by name, unique identifier (UID), or instance.

For a machine to be used in a site, the machine must be added to a desktop group. The machine and desktop group must be compatible in order for the process to succeed; for example a machine in a single-session catalog cannot be added to a multi-session desktop group.

For more information about machines, see about_Broker_Machines.

Related topics

Add-BrokerMachinesToDesktopGroup

Remove-BrokerMachine

Get-BrokerMachine

Parameters

-InputObject<Machine[]>

An array of machines to add to the group.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MachineName<String>

The name of the single machine to add (must match the MachineName property of the machine).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroup<DesktopGroup>

The desktop group to which the machines are added, specified by name, Uid, or instance.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Machine You can pipe in the machines you want to add.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Add-BrokerMachine -InputObject $machine -DesktopGroup $desktopGroup
C:\PS> Add-BrokerMachine -InputObject $machine -DesktopGroup 2
C:\PS> Add-BrokerMachine $machine -DesktopGroup "MyDesktopGroup"
```

These examples all add a single machine instance to a desktop group, identifying the group by instance, UID, or name.

---------- EXAMPLE 2 ----------

```
C:\PS> Add-BrokerMachine -MachineName "MyDomain\MyMachine" -DesktopGroup 2
C:\PS> Add-BrokerMachine "MyDomain\MyMachine" -DesktopGroup "MyDesktopGroup"
C:\PS> Add-BrokerMachine "MyDomain\MyMachine" -DesktopGroup $desktopGroup
```

These examples add the machine called MyMachine to a desktop group.

---------- EXAMPLE 3 ----------

```
C:\PS> Get-BrokerMachine -Uid 3 | Add-BrokerMachine -DesktopGroup 2
C:\PS> Get-BrokerMachine -CatalogUid 4 | Add-BrokerMachine -DesktopGroup 2
```

These examples find specific machines and add them to a desktop group.

Add-BrokerMachineConfiguration

Sep 10, 2014

Adds a machine configuration to a desktop group.

Syntax

```
Add-BrokerMachineConfiguration [-InputObject] <MachineConfiguration[]> [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-BrokerMachineConfiguration [-Name] <String> [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Associates a machine configuration with a desktop group. The settings in the machine configuration are then applied to the machines in the desktop group.

Related topics

New-BrokerMachineConfiguration

Set-BrokerMachineConfiguration

Rename-BrokerMachineConfiguration

Remove-BrokerMachineConfiguration

Parameters

-InputObject<MachineConfiguration[]>

Machine configuration to add to the desktop group.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Name of a machine configuration to add to the desktop group.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroup<DesktopGroup>

The desktop group to which the machine configurations are added, specified by name, Uid, or instance.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.MachineConfiguration The machine configuration to add to the desktop group.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
Add-BrokerMachineConfiguration -Name UPM\Conf1 -DesktopGroup 1
```

Adds the machine configuration named UPM\Conf1 to the desktop group with Uid 1.

---------- EXAMPLE 2 ----------

```
$mc | Add-BrokerMachineConfiguration -DesktopGroup AdminDesktops
```

Adds the machine configuration $mc to the desktop group named "AdminDesktops".

Add-BrokerMachinesToDesktopGroup

Sep 10, 2014

Adds machines from a catalog to a desktop group.

Syntax

```
Add-BrokerMachinesToDesktopGroup [-Catalog] <Catalog> [-DesktopGroup] <DesktopGroup> [-Count] <Int32> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Add-BrokerMachinesToDesktopGroup cmdlet adds a specified number of machines from a catalog to a desktop group.

The cmdlet adds as many machines as possible from the catalog to the desktop group, up to the specified number. The number of machines successfully added to the desktop group is returned.

The machines are added randomly from the catalog and are selected from those that are not already members of a desktop group, and not already assigned to a client, IP address, or user.

Both the catalog and desktop group can be referenced either by instance, name, or unique identifier (Uid). The allocation type of the catalog must be compatible with the type of desktop group. This means the session support (single/multi) and the allocation type (private/shared) of the catalog must match the session support and allocation type in the desktop group.

Related topics

Add-BrokerMachine

Remove-BrokerMachine

Parameters

-Catalog<Catalog>

The catalog from which the machines are taken.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroup<DesktopGroup>

The desktop group to which the machines are added.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Count<Int32>

The number of machines to add to the desktop group.

Required?	true

Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Catalog, or the name or Uid of the catalog. You can pipe in the catalog from which the machines are taken. Alternatively, you can pipe the name or the Uid of the catalog.

Return Values

System.Int32

The number of machines added to the desktop group.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Add-BrokerMachinesToDesktopGroup -Catalog $catalog -DesktopGroup $desktopGroup -Count 1000
C:\PS> Add-BrokerMachinesToDesktopGroup -Catalog "MyCatalog" -DesktopGroup "MyDesktopGroup" -Count 1000
C:\PS> Add-BrokerMachinesToDesktopGroup -Catalog 23 -DesktopGroup 4 -Count 1000
```

All these examples request that a thousand machines from a catalog are added to a desktop group. The first example references both catalog and desktop group by instance. The second example references both catalog and desktop group by name. The third example references both catalog and desktop group by Uid.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerCatalog -ProvisioningType Manual | Add-BrokerMachinesToDesktopGroup -DesktopGroup $desktopGroup -Count 10
```

This example takes ten machines from each manually provisioned catalog and adds them to the specified desktop group.

Add-BrokerScope

Sep 10, 2014

Add the specified catalog/desktop group to the given scope(s).

Syntax

Add-BrokerScope [-InputObject] <Scope[]> [-Catalog <Catalog>] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Add-BrokerScope cmdlet is used to associate a catalog or desktop group object with given scope(s).

To add a catalog/desktop group to a scope you need permission to change the scopes of the catalog/desktop group and permission to add objects to all of the scopes you have specified.

If the catalog/desktop group is already in any scope supplied, that scope will be silently ignored.

Related topics

Parameters

-InputObject<Scope[]>

Specifies the scope(s) to add the object to. Each can take the form of either the string form of the scope's GUID or its name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Catalog<Catalog>

Specifies the catalog object to be added. This can take the form of an existing catalog object, a catalog Uid or name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroup<DesktopGroup>

Specifies the desktop group object to be added. This can take the form of an existing desktop group object, a desktop

group Uid or name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Scope You can pipe scopes to Add-BrokerScope.

Return Values

NONE

Examples

---------- EXAMPLE 1 ----------

C:\PS> Add-BrokerScope -Scope Chalfont –DesktopGroup 27
Adds the desktop group with Uid 27 to the Chalfont scope.

---------- EXAMPLE 2 ----------

C:\PS> Add-BrokerScope BFC74867-C6EF-482C-996F-3E0D340E96AC -Catalog BangaloreMachines

Adds the BangaloreMachines catalog to the scope with the specified ScopeID.

Add-BrokerTag

Sep 10, 2014

Associate a tag with another object.

Syntax

Add-BrokerTag [-InputObject] <Tag[]> [-Desktop <Desktop>] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-BrokerTag [-Name] <String> [-Desktop <Desktop>] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Associates one or more tags with another object.

Related topics

Get-BrokerTag

New-BrokerTag

Remove-BrokerTag

Rename-BrokerTag

Parameters

-InputObject<Tag[]>

Specifies one or more tag objects.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies a tag by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Desktop<Desktop>

Associates the tag with a desktop.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroup<DesktopGroup>

Associates the tag with a desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.

Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Tag Tags may be specified through pipeline input.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $desktop = Get-BrokerDesktop -Uid 1
C:\PS> Add-BrokerTag -Name 'Tag1' -Desktop $desktop
```

Associates 'Tag1' with Desktop $desktop.

---------- EXAMPLE 2 ----------

```
C:\PS> $desktop = Get-BrokerDesktop -Uid 1
C:\PS> New-BrokerTag 'Tag2' | Add-BrokerTag -Desktop $desktop
```

Creates a new tag with name 'Tag2' and associates it with Desktop $desktop.

Add-BrokerUser

Sep 10, 2014

Creates an association between a user and another broker object

Syntax

Add-BrokerUser [-InputObject] <User[]> [-Application <Application>] [-SessionLinger <SessionLinger>] [-SessionPreLaunch <SessionPreLaunch>] [-Machine <Machine>] [-PrivateDesktop <PrivateDesktop>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-BrokerUser [-Name] <String> [-Application <Application>] [-SessionLinger <SessionLinger>] [-SessionPreLaunch <SessionPreLaunch>] [-Machine <Machine>] [-PrivateDesktop <PrivateDesktop>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Add-BrokerUser cmdlet adds broker user objects to another specified object, such as a broker private desktop. This depends on the target object type:

o Machine - assign the broker machine to the specified user(s); when the machine is subsequently added to a desktop group, the desktop is also assigned to the same user(s).

o PrivateDesktop - assign the desktop to the specified user(s).

o Application - assign the application to the specified user(s).

Related topics

Get-BrokerUser

Remove-BrokerUser

Parameters

-InputObject<User[]>

The user objects to add.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the user or users to be added.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-Application<Application>

The application to which the user is to be associated.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-SessionLinger<SessionLinger>

The session linger setting to which the user is to be assigned.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByValue)

-SessionPreLaunch<SessionPreLaunch>

The session pre-launch setting to which the user is to be assigned.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByValue)

-Machine<Machine>

The machine to which the user is to be assigned

Required?	false

Default Value	null
Accept Pipeline Input?	true (ByValue)

-PrivateDesktop<PrivateDesktop>

The desktop to which the user is to be assigned

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.USer You can pipe the users to be added to Add-BrokerUser.

Return Values

None

Notes

Specify one of the -Machine or -PrivateDesktop or -Application parameters only.

Examples

---------- EXAMPLE 1 ----------

```
Add-BrokerUser "DOMAIN\UserName" -PrivateDesktop "DOMAIN\MachineName"
```

Assign the specified private desktop to the specified user.

---------- EXAMPLE 2 ----------

```
Add-BrokerUser "DOMAIN\UserName" -Application "ApplicationName"
```

Assign the specified application to the specified user.

---------- EXAMPLE 3 ----------

```
Add-BrokerUser "DOMAIN\UserName" -Application "FolderName"\"ApplicationName"
```

Assign the specified application, in the specified folder, to the specified user.

Disconnect-BrokerSession

Sep 10, 2014

Disconnect a session.

Syntax

```
Disconnect-BrokerSession [-InputObject] <Session[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Disconnects the specified session.

If the session is active, no warning is issued to the user before that session is disconnected.

After disconnection, sessions enter a Disconnected state. In a Disconnected state, a session still exists but there is no remote connection to that session.

Related topics

Get-BrokerSession

Stop-BrokerSession

Parameters

-InputObject<Session[]>

Identifies the session(s) to disconnect. This can be expressed as either a session Uid or a session object.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Session The sessions to disconnect can be piped into this cmdlet.

Return Values

None

Notes

This operation is non-blocking and returns before it completes. The operation, however, is unlikely to fail unless there are communication problems between the controller and the machine, or if bad arguments are passed to the cmdlet itself or if the machine cannot successfully execute the operation.

The transient nature of sessions means that the list of session objects or UIDs supplied to Disconnect-BrokerSession could consist of valid and invalid sessions. Invalid sessions are detected and disregarded and the disconnect session operation is invoked on only the valid sessions.

The system can fail to disconnect the session if the machine is not in an appropriate state or if there are problems in communicating with the machine. When a disconnect is requested the system detects if the operation was initiated successfully or not by the machine. As this operation is non-blocking the system doesn't detect or report whether the disconnect ultimately succeeded or failed after it was started.

Disconnect failures are reported through the broker SDK error handling mechanism (see about_Broker_ErrorHandling). In the event of errors the SdkErrorRecord error status is set to SessionOperationFailed and its error data dictionary is populated with the following entries:

o OperationsAttemptedCount: The number of operations attempted.

o OperationsFailedCount - The number of failed operations.

o OperationsSucceededCount - The number of successfully executed operations.

o UnresolvedSessionFailuresCount - The number of operations that failed due to invalid sessions being supplied.

o OperationInvocationFailuresCount - The number of operations that failed because they could not be invoked on the machine.

o DesktopExecutionFailuresCount - The number of operations that failed because they could not be successfully executed by the machine.

The SdkErrorRecord message will also display the number of attempted, failed and successful operations in the following format:

"Session operation error - attempted:<OperationsAttemptedCount>, failed:<OperationsFailedCount>, succeeded:<OperationsSucceededCount>"

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS> Get-BrokerSession -UserName MyDomain\MyAccount | Disconnect-BrokerSession
```

Attempts to disconnect all of the sessions for the user MyDomain\MyAccount.

-------------------------- EXAMPLE 2 --------------------------

```
C:\PS> $desktop = Get-BrokerDesktop -DNSName MyMachine.MyDomain.com
C:\PS> Disconnect-BrokerSession $desktop.SessionUid
```

Disconnects the session on MyMachine.

-------------------------- EXAMPLE 3 --------------------------

```
C:\PS> trap  [Citrix.Broker.Admin.SDK.SdkOperationException]
C:\PS> {
C:\PS>   write $("Exception name = " + $_.Exception.GetType().FullName)
C:\PS>   write $("SdkOperationException.Status = " + $_.Exception.Status)
C:\PS>   write $("SdkOperationException.ErrorData=")
C:\PS>   $_.Exception.ErrorData
C:\PS>
C:\PS>   write $("SdkOperationException.InnerException = " + $_.Exception.InnerException)
C:\PS>   $_.Exception.InnerException
C:\PS>   continue
C:\PS> }
C:\PS>
C:\PS> Disconnect-BrokerSession -InputObject 10,11,12
```

Attempts to disconnect sessions 10, 11 and 12. Traps and displays the error information.

Export-BrokerDesktopPolicy

Sep 10, 2014

Gets the site wide Citrix Group Policy settings.

Syntax

```
Export-BrokerDesktopPolicy [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Export-BrokerDesktopPolicy returns an array of bytes containing the site-wide Citrix Group Policy settings. These policy settings are applied to every machine in the site.

Related topics

Import-BrokerDesktopPolicy

New-BrokerConfigurationSlot

New-BrokerMachineConfiguration

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None

Return Values

System.Byte[]

The configuration data as an opaque binary blob. This will be null if no site wide Citrix Group Policy settings are in place.

Notes

Export-BrokerDesktopPolicy performs a specialized operation. Direct usage of it in scripts is discouraged, and could result in data corruption. It is recommended that this operation only be performed via the Citrix Studio.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $policy = Export-BrokerDesktopPolicy
```

This command exports the site wide Citrix Group Policy settings.

Get-BrokerAccessPolicyRule

Sep 10, 2014

Gets rules from the site's access policy.

Syntax

Get-BrokerAccessPolicyRule [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerAccessPolicyRule [[-Name] <String>] [-AllowedConnections <AllowedConnection>] [-AllowedUsers <AllowedUser>] [-Description <String>] [-DesktopGroupName <String>] [-DesktopGroupUid <Int32>] [-Enabled <Boolean>] [-ExcludedClientIPFilterEnabled <Boolean>] [-ExcludedClientName <String>] [-ExcludedClientNameFilterEnabled <Boolean>] [-ExcludedSmartAccessFilterEnabled <Boolean>] [-ExcludedSmartAccessTag <String>] [-ExcludedUser <User>] [-ExcludedUserFilterEnabled <Boolean>] [-IncludedClientIPFilterEnabled <Boolean>] [-IncludedClientName <String>] [-IncludedClientNameFilterEnabled <Boolean>] [-IncludedSmartAccessFilterEnabled <Boolean>] [-IncludedSmartAccessTag <String>] [-IncludedUser <User>] [-IncludedUserFilterEnabled <Boolean>] [-Metadata <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns rules matching the specified search criteria from the site's access policy. If no search criteria are specified, all rules in the access policy are obtained.

An access policy rule defines a set of connection filters and access control rights relating to a desktop group. These allow fine-grained control of what access is granted to a desktop group based on details of, for example, a user's endpoint device, its address, and the user's identity.

---------- BrokerAccessPolicyRule Object

A BrokerAccessPolicyRule object represents a single rule within the site's access policy. For a user to gain access to a desktop group via the rule their connection must match all its enabled include filters, and none of its enabled exclude filters. The object contains the following properties:

-- AllowedConnections (Citrix.Broker.Admin.SDK.AllowedConnection)

Controls whether connections must be local or via Access Gateway, and if so whether specified SmartAccess tags must be provided by Access Gateway with the connection. This property forms part of the included SmartAccess tags filter.

For a detailed description of this property see "help about_Broker_AccessPolicy".

-- AllowedProtocols (System.String[])

Protocols (for example HDX, RDP) available to the user for sessions delivered from the rule's desktop group. If the user gains access to a desktop group by multiple rules, the allowed protocol list is the combination of the protocol lists from all those rules.

If the protocol list is empty, access to the desktop group is implicitly denied.

-- AllowedUsers (Citrix.Broker.Admin.SDK.AllowedUser)

Controls the behavior of the included users filter. This can restrict access to a list of named users or groups, or allow access to any authenticated user. For a detailed description of this property see "help about_Broker_AccessPolicy".

-- AllowRestart (System.Boolean)

Indicates if the user can restart sessions delivered from the rule's desktop group. Session restart is handled as follows: For sessions on single-session power-managed machines, the machine is powered off, and a new session launch request made; for sessions on multi-session machines, a logoff request is issued to the session, and a new session launch request made; otherwise the property is ignored.

-- Description (System.String)

An optional description of the rule. The text is purely informational for the administrator, it is never visible to the end user.

-- DesktopGroupName (System.String)

The name of the desktop group to which the rule applies.

-- DesktopGroupUid (System.Int32)

The unique ID of the desktop group to which the rule applies.

-- Enabled (System.Boolean)

Indicates whether the rule is enabled. A disabled rule is ignored when evaluating the site's access policy.

-- ExcludedClientIPFilterEnabled (System.Boolean)

Indicates whether the excluded client IP filter is enabled. If the filter is disabled it is ignored when the rule is evaluated.

-- ExcludedClientIPs (Citrix.Broker.Admin.SDK.ChbIPAddressRange[])

IP addresses of user devices explicitly denied access to the rule's desktop group. Addresses can be specified as simple numeric addresses or as subnet masks (for example, 10.40.37.5 or 10.40.0.0/16). This property forms part of the excluded client IP address filter.

-- ExcludedClientNameFilterEnabled (System.Boolean)

Indicates whether the excluded client name filter is enabled. If the filter is disabled it is ignored when the rule is evaluated.

-- ExcludedClientNames (System.String[])

Names of user devices explicitly denied access to the rule's desktop group. This property forms part of the excluded client names filter.

-- ExcludedSmartAccessFilterEnabled (System.Boolean)

Indicates whether the excluded SmartAccess tags filter is enabled. If the filter is disabled it is ignored when the rule is evaluated.

-- ExcludedSmartAccessTags (System.String[])

SmartAccess tags which explicitly deny access to the rule's desktop group if any occur in those provided by Access Gateway

with the user's connection. This property forms part of the excluded SmartAccess tags filter.

-- ExcludedUserFilterEnabled (System.Boolean)

Indicates whether the excluded users filter is enabled. If the filter is disabled it is ignored when the rule is evaluated.

-- ExcludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

Users and groups who are explicitly denied access to the rule's desktop group. This property forms part of the excluded users filter.

-- HdxSslEnabled (System.Boolean)

Indicates whether SSL encryption is enabled for sessions delivered from the rule's desktop group.

-- IncludedClientIPFilterEnabled (System.Boolean)

Indicates whether the included client IP filter is enabled. If the filter is disabled it is ignored when the rule is evaluated.

-- IncludedClientIPs (Citrix.Broker.Admin.SDK.ChbIPAddressRange[])

IP addresses of user devices allowed access to the rule's desktop group. Addresses can be specified as simple numeric addresses or as subnet masks (for example, 10.40.37.5 or 10.40.0.0/16). This property forms part of the included client IP address filter.

-- IncludedClientNameFilterEnabled (System.Boolean)

Indicates whether the included client names filter is enabled. If the filter is disabled it is ignored when the rule is evaluated.

-- IncludedClientNames (System.String[])

Names of user devices allowed access to the rule's desktop group. This property forms part of the included client names filter.

-- IncludedSmartAccessFilterEnabled (System.Boolean)

Indicates whether the included SmartAccess tags filter is enabled. If the filter is disabled it is ignored when the rule is evaluated.

-- IncludedSmartAccessTags (System.String[])

The SmartAccess tags which grant access to the rule's desktop group if any occur in those provided by Access Gateway with the user's connection. This property forms part of the excluded SmartAccess tags filter.

-- IncludedUserFilterEnabled (System.Boolean)

Indicates whether the included users filter is enabled. If the filter is disabled it is ignored when the rule is evaluated.

-- IncludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

Users and groups who are granted access to the rule's desktop group. This property forms part of the included users filter.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

A collection of arbitrary key/value pairs that can be associated with the rule. The administrator can use these values for any

purpose; they are not used by the site itself in any way.

-- Name (System.String)

Administrative name of the rule. Each rule in the site's access policy must have a unique name.

-- Uid (System.Int32)

Unique ID of the rule itself.

Related topics

New-BrokerAccessPolicyRule

Set-BrokerAccessPolicyRule

Rename-BrokerAccessPolicyRule

Remove-BrokerAccessPolicyRule

Parameters

-Uid<Int32>

Gets only the rule with the specified unique ID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets only rules with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AllowedConnections<AllowedConnection>

Gets only rules that have the specified value in the AllowedConnections property of their included SmartAccess tags filter.

Valid values are Filtered, NotViaAG, and ViaAG.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AllowedUsers<AllowedUser>

Gets only rules that have the specified value in the AllowedUsers property of their included users filter.

Valid values are Filtered, AnyAuthenticated, Any, AnonymousOnly and FilteredOrAnonymous.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets only rules with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets only rules applying to desktop groups with names matching the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets only rules that apply to the desktop group with the specified unique ID.

Required?	false

Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets only rules that are in the specified state, either enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedClientIPFilterEnabled<Boolean>

Gets only rules that have their excluded client IP address filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedClientName<String>

Gets only rules that have the specified client name in their excluded client names filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedClientNameFilterEnabled<Boolean>

Gets only rules that have their excluded client name filter enabled ($true) or disabled ($false).

Required?	false

Default Value	
Accept Pipeline Input?	false

-ExcludedSmartAccessFilterEnabled<Boolean>

Gets only rules that have their excluded SmartAccess tags filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedSmartAccessTag<String>

Gets only rules that have the specified SmartAccess tag in their excluded SmartAccess tags filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUser<User>

Gets only rules that have the specified user in their excluded users filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Gets only rules that have their excluded user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	

Accept Pipeline Input?	false

-IncludedClientIPFilterEnabled<Boolean>

Gets only rules that have their included client IP address filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedClientName<String>

Gets only rules that have the specified user device name in their included client names filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedClientNameFilterEnabled<Boolean>

Gets only rules that have their included client name filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedSmartAccessFilterEnabled<Boolean>

Gets only rules that have their included SmartAccess tags filter enabled ($true) or disabled ($false).

Required?	false
Default Value	

Accept Pipeline Input?	false

-IncludedSmartAccessTag<String>

Gets only rules that have the specified SmartAccess tag in their included SmartAccess tags filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUser<User>

Gets only rules that have the specified user in their included users filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Gets only rules that have their included user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false

Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.AccessPolicyRule

Get-BrokerAccessPolicyRule returns all access policy rules that match the specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerAccessPolicyRule
Returns all access policy rules. This offers a complete description of the current site's access policy.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerAccessPolicyRule -Enabled $true -IncludedUser sales\tech-support
Returns all rules that are both enabled and explicitly include the SALES\tech-support group in their included users filter.

Get-BrokerAdminFolder

Sep 10, 2014

Get the admin folders in this site.

Syntax

```
Get-BrokerAdminFolder [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>]
[<CommonParameters>]

Get-BrokerAdminFolder [[-Name] <String>] [-DirectChildAdminFolders <Int32>] [-DirectChildApplications
<Int32>] [-FolderName <String>] [-LastChangeId <Guid>] [-Metadata <String>] [-ParentAdminFolderUid
<Int32>] [-TotalChildApplications <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip
<Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

The Get-BrokerAdminFolder cmdlet gets admin folders in this site.

Without parameters, Get-BrokerAdminFolder gets all the admin folders that have been created. You can also use the parameters of Get-BrokerAdminFolder to filter the results to just the folders you're interested in. You can also identify folders by their UIDs or their FolderNames.

---------- BrokerAdminFolder Object

A folder for use in the administration console for organising other objects. E.g. BrokerApplication objects

-- DirectChildAdminFolders (System.Int32)

The number of admin folders with this folder as a direct parent

-- DirectChildApplications (System.Int32)

The number of applications in this admin folder (does not include any applications in child folders)

-- FolderName (System.String)

The simple name of this folder within any parent folder

-- LastChangeId (System.Guid)

A random GUID assigned whenever there is a change anywhere in the hierarchy of admin folders below this node; each change updates this value on the changed folder and all parents all the way up to the root folder. Note that nodes below any change do not have their LastChangeId value updated

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Holds any metadata associated with the admin folder

-- Name (System.String)

The full name of the folder including the full parent hierarchy separated by back-slash characters and including a trailing

back-slash

-- ParentAdminFolderUid (System.Int32)

The UID of the parent admin folder; the root folder references itself (zero)

-- TotalChildApplications (System.Int32)

The number of applications in this admin folder (including any applications in child folders)

-- Uid (System.Int32)

The unique ID of the admin folder (the root folder has the value zero)

Related topics

New-BrokerAdminFolder

Remove-BrokerAdminFolder

Parameters

-Uid<Int32>

Gets only the admin folder with the specified unique identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets admin folders matching the specified name (if no trailing backslash is supplied, it is assumed).

Required?	false
Default Value	
Accept Pipeline Input?	false

-DirectChildAdminFolders<Int32>

Gets admin folders with the specified number of child folders.

Required?	false

Default Value	
Accept Pipeline Input?	false

-DirectChildApplications<Int32>

Gets admin folders with the specified number of applications (excluding those in sub-folders).

Required?	false
Default Value	
Accept Pipeline Input?	false

-FolderName<String>

Gets only the admin folders matching the specified simple folder name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastChangeId<Guid>

Gets only the admin folders with the specified value for LastChangeId.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false

Default Value	
Accept Pipeline Input?	false

-ParentAdminFolderUid<Int32>

Gets only admin folders with the specified parent admin folder UID value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TotalChildApplications<Int32>

Gets admin folders with the specified number of applications (including those in sub-folders).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false

Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None Input cannot be piped to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.AdminFolder

Returns admin folders.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerAdminFolder
```

Return all administration folders.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerAdminFolder -Uid 1
```

Get the administration folder with Uid 1.

Get-BrokerAppAssignmentPolicyRule

Sep 10, 2014

Gets application rules from the site's assignment policy.

Syntax

```
Get-BrokerAppAssignmentPolicyRule [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerAppAssignmentPolicyRule [[-Name] <String>] [-Description <String>] [-DesktopGroupUid <Int32>] [-Enabled <Boolean>] [-ExcludedUser <User>] [-ExcludedUserFilterEnabled <Boolean>] [-IncludedUser <User>] [-IncludedUserFilterEnabled <Boolean>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns application rules matching the specified search criteria from the site's assignment policy. If no search criteria are specified, all application rules in the assignment policy are obtained.

An application rule in the assignment policy defines the users who are entitled to a self-service persistent machine assignment from the rule's desktop group; once assigned the machine can run one or more applications published from the group.

---------- BrokerAppAssignmentPolicyRule Object

The BrokerAppAssignmentPolicyRule object represents a single application rule within the site's assignment policy. It contains the following properties:

-- Description (System.String)

An optional description of the rule. The text is purely informational for the administrator, it is never visible to the end user.

-- DesktopGroupUid (System.Int32)

The unique ID of the desktop group to which the rule applies.

-- Enabled (System.Boolean)

Indicates whether the rule is enabled. A disabled rule is ignored when evaluating the site's assignment policy.

-- ExcludedUserFilterEnabled (System.Boolean)

Indicates whether the excluded users filter is enabled. If the filter is disabled then any user entries in the filter are ignored when assignment policy rules are evaluated.

-- ExcludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

The excluded users filter of the rule, that is, the users and groups who are explicitly denied an entitlement to a machine assignment from the rule's desktop group.

-- IncludedUserFilterEnabled (System.Boolean)

Indicates whether the included users filter is enabled. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly entitled to the machine assignment described by the rule.

-- IncludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

The included users filter of the rule, that is, the users and groups who are entitled to a machine assignment from the rule's desktop group.

-- Name (System.String)

The administrative name of the rule. Each rule in the site's assignment policy must have a unique name (irrespective of whether they are desktop or application rules).

-- Uid (System.Int32)

The unique ID of the rule itself.

Related topics

New-BrokerAppAssignmentPolicyRule

Set-BrokerAppAssignmentPolicyRule

Rename-BrokerAppAssignmentPolicyRule

Remove-BrokerAppAssignmentPolicyRule

Parameters

-Uid<Int32>

Gets the application rule with the specified unique ID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets only application rules with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets only application rules with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets only application rules that apply to the desktop group with the specified unique ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets only application rules that are in the specified state, either enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUser<User>

Gets only application rules that have the specified user in their excluded users filter (whether the filter is enabled or not)

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Gets only application rules that have their excluded user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUser<User>

Gets only application rules that have the specified user in their included users filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Gets only application rules that have their included user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.AppAssignmentPolicyRule

Get-BrokerAppAssignmentPolicyRule returns all application rules in the assignment policy that match the specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerAppAssignmentPolicyRule
```

Returns all application rules from the assignment policy. This offers a complete description of the current site's assignment policy with respect to machine assignment entitlements for delivery of application sessions from private desktop groups.

---------- EXAMPLE 2 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Sales Support'
C:\PS> Get-BrokerAppAssignmentPolicyRule -DesktopGroupUid $dg.Uid
```

Returns the rule in the assignment policy that gives users entitlements to machine assignments in the Sales Support

desktop group for delivery of application sessions.

Get-BrokerAppEntitlementPolicyRule

Sep 10, 2014

Gets application rules from the site's entitlement policy.

Syntax

Get-BrokerAppEntitlementPolicyRule [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerAppEntitlementPolicyRule [[-Name] <String>] [-Description <String>] [-DesktopGroupUid <Int32>] [-Enabled <Boolean>] [-ExcludedUser <User>] [-ExcludedUserFilterEnabled <Boolean>] [-IncludedUser <User>] [-IncludedUserFilterEnabled <Boolean>] [-SessionReconnection <SessionReconnection>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns application rules matching the specified search criteria from the site's entitlement policy. If no search criteria are specified, all application rules in the entitlement policy are obtained.

An application rule in the entitlement policy defines the users who are allowed per-session access to a machine to run one or more applications published from the rule's desktop group.

---------- BrokerAppEntitlementPolicyRule Object

The BrokerAppEntitlementPolicyRule object represents a single application rule within the site's entitlement policy. It contains the following properties:

-- Description (System.String)

Optional description of the rule. The text is purely informational for the administrator, it is never visible to the end user.

-- DesktopGroupUid (System.Int32)

The unique ID of the desktop group to which the rule applies.

-- Enabled (System.Boolean)

Indicates whether the rule is enabled. A disabled rule is ignored when evaluating the site's entitlement policy.

-- ExcludedUserFilterEnabled (System.Boolean)

Indicates whether the excluded users filter of the rule is enabled. If the filter is disabled then any user entries in the filter are ignored when entitlement policy rules are evaluated.

-- ExcludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

The excluded users filter of the rule, that is, the users and groups who are explicitly denied entitlements to use published applications from the associated desktop group.

-- IncludedUserFilterEnabled (System.Boolean)

Indicates whether the included users filter of the rule is enabled. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to an application session by the rule.

-- IncludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

The included users filter of the rule, that is, the users and groups who are granted an entitlement to an application session by the rule.

If a user appears explicitly in the excluded users filter of the rule or is a member of a group that appears in the excluded users filter, no entitlement is granted whether or not the user appears in the included users filter.

-- Name (System.String)

The administrative name of the rule. Each rule in the site's entitlement policy must have a unique name (irrespective of whether they are desktop or application rules).

-- SessionReconnection (Citrix.Broker.Admin.SDK.SessionReconnection)

Defines reconnection (roaming) behavior for sessions launched using this rule. Session reconnection control is an experimental and unsupported feature.

-- Uid (System.Int32)

The unique ID of the rule itself.

Related topics

New-BrokerAppEntitlementPolicyRule

Set-BrokerAppEntitlementPolicyRule

Rename-BrokerAppEntitlementPolicyRule

Remove-BrokerAppEntitlementPolicyRule

Parameters

-Uid<Int32>

Gets the application rule with the specified unique ID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets only application rules with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets only application rules with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets only the application rule that applies to the desktop group with the specified unique ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets only application rules that are in the specified state, either enabled ($true), or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUser<User>

Gets only application rules that have the specified user in their excluded users filter (whether the filter is enabled or not).

Required?	false

Default Value	
Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Gets only application rules that have their excluded user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUser<User>

Gets only application rules that have the specified user in their included users filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Gets only application rules that have their included user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionReconnection<SessionReconnection>

Gets only application rules with the specified session reconnection behavior.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false

Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.AppEntitlementPolicyRule

Get-BrokerAppEntitlementPolicyRule returns all application rules from the entitlement policy that match the specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerAppEntitlementPolicyRule
```

Returns all application rules from the entitlement policy. This offers a complete description of the current site's entitlement policy with respect to application entitlements from shared desktop groups.

---------- EXAMPLE 2 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Customer Support'
C:\PS> Get-BrokerAppEntitlementPolicyRule -DesktopGroupUid $dg.Uid
```

Returns the application rule in the entitlement policy that grants users an entitlement to application sessions in the Customer Support desktop group.

Get-BrokerApplication

Sep 10, 2014

Get the applications published on this site.

Syntax

Get-BrokerApplication [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerApplication [[-Name] <String>] [-AdminFolderName <String>] [-AdminFolderUid <Int32>] [-ApplicationName <String>] [-ApplicationType <ApplicationType>] [-AssociatedDesktopGroupPriority <Int32>] [-AssociatedDesktopGroupUid <Int32>] [-AssociatedDesktopGroupUUID <Guid>] [-AssociatedUserFullName <String>] [-AssociatedUserName <String>] [-AssociatedUserUPN <String>] [-BrowserName <String>] [-ClientFolder <String>] [-CommandLineArguments <String>] [-CommandLineExecutable <String>] [-CpuPriorityLevel <CpuPriorityLevel>] [-Description <String>] [-Enabled <Boolean>] [-IconFromClient <Boolean>] [-IconUid <Int32>] [-MetadataKey <String>] [-Metadata <String>] [-PublishedName <String>] [-SecureCmdLineArgumentsEnabled <Boolean>] [-ShortcutAddedToDesktop <Boolean>] [-ShortcutAddedToStartMenu <Boolean>] [-StartMenuFolder <String>] [-UserFilterEnabled <Boolean>] [-UUID <Guid>] [-Visible <Boolean>] [-WaitForPrinterCreation <Boolean>] [-WorkingDirectory <String>] [-DesktopUid <Int32>] [-SessionUid <Int64>] [-UserSID <String>] [-DesktopGroupUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Get-BrokerApplication cmdlet gets the published applications that are hosted on this site.

Without parameters, Get-BrokerApplication gets all the applications that have been published, regardless of whether they are visible to users or not. You can also use the parameters of Get-BrokerApplication to filter the results to just the applications you're interested in. You can also identify applications by their UIDs or their BrowserNames.

For more information about applications, see about_Broker_Applications.

---------- BrokerApplication Object

The BrokerApplication object represents a published application in the site. It contains the following properties:

-- AdminFolderName (System.String)

The name of the admin folder the application is in (including trailing backslash), or the empty string if the application is at the root level

-- AdminFolderUid (System.Int32)

The Uid of the admin folder the application is in (if any)

-- ApplicationName (System.String)

The simple name of the application within its parent admin folder (if any)

-- ApplicationType (Citrix.Broker.Admin.SDK.ApplicationType)

The type of the application, whether HostedOnDesktop or InstalledOnClient.

-- AssociatedDesktopGroupPriorities (System.Int32[])

List of associated desktop group priorities. Associated desktop groups is the list of desktop groups on which the application is published. When launching an application an available machine from one of the associated groups is selected. Desktop groups are searched for available machines in order of their priority.

-- AssociatedDesktopGroupUids (System.Int32[])

List of associated desktop group uids. Associated desktop groups is the list of desktop groups on which the application is published. The list is sorted by priority, with the highest priority group first.

-- AssociatedDesktopGroupUUIDs (System.Guid[])

List of associated desktop group UUIDs. Associated desktop groups is the list of desktop groups on which the application is published. The list is sorted by priority, with the highest priority group first.

-- AssociatedUserFullNames (System.String[])

List of associated users (full names). Associated users is the list of users who are given access using the application/user mapping filter.

-- AssociatedUserNames (System.String[])

List of associated users (SAM names). Associated users is the list of users who are given access using the application/user mapping filter.

-- AssociatedUserUPNs (System.String[])

List of associated users (user principle names). Associated users is the list of users who are given access using the application/user mapping filter.

-- BrowserName (System.String)

Unique browser name used to identify this application to other components in the site. This value is not visible to the end users.

-- ClientFolder (System.String)

The folder that the application belongs to as the user sees it.

-- CommandLineArguments (System.String)

The command-line arguments to use when launching the executable.

-- CommandLineExecutable (System.String)

The name including the full path of the executable file to launch.

-- CpuPriorityLevel (Citrix.Broker.Admin.SDK.CpuPriorityLevel)

The CPU priority of the launched process. Valid values are: Low, BelowNormal, Normal, AboveNormal, and High.

-- Description (System.String)

Optional application description. This description is visible to the end users.

-- Enabled (System.Boolean)

Specifies whether or not this application can be launched.

-- IconFromClient (System.Boolean)

Specifies if the app icon should be retrieved from the application on the client. This is reserved for possible future use, and all applications of type HostedOnDesktop cannot set or change this value.

-- IconUid (System.Int32?)

The icon UID used for this application. If not specified a generic icon is used.

-- MetadataKeys (System.String[])

All key names of metadata items associated with this application.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Metadata for this application.

-- Name (System.String)

Unique administrative name of application; this will include any parent admin folder hierarchy separated by backslash characters.

-- PublishedName (System.String)

Published name of application as seen by end user. If not specified value used defaults to the administrative name.

-- SecureCmdLineArgumentsEnabled (System.Boolean)

Specifies whether the command-line arguments should be secured.

-- ShortcutAddedToDesktop (System.Boolean)

Specifies whether a shortcut to the application should be placed on the user device.

-- ShortcutAddedToStartMenu (System.Boolean)

Specifies whether a shortcut to the application should be placed in the user's Start menu on their user device.

-- StartMenuFolder (System.String)

The name of the Start menu folder that holds the application shortcut.

-- Uid (System.Int32)

A unique identifier of an application.

-- UserFilterEnabled (System.Boolean)

Indicates if application-specific user filter is enabled.

-- UUID (System.Guid)

UUID of the application.

-- Visible (System.Boolean)

Specifies if the application is visible to users.

-- WaitForPrinterCreation (System.Boolean)

Specifies whether the VDA delays starting the app until printers are set up or not.

-- WorkingDirectory (System.String)

The working directory the executable is launched from.

Related topics

New-BrokerApplication

Add-BrokerApplication

Remove-BrokerApplication

Rename-BrokerApplication

Move-BrokerApplication

Set-BrokerApplication

Parameters

-Uid<Int32>

Gets only the application with the specified unique identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets only the applications matching the specified name (including any parent admin folder hierarchy.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminFolderName<String>

Gets applications that are in admin folders matching the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminFolderUid<Int32>

Gets applications that are in the specified admin folder.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationName<String>

Gets applications that match the specified simple name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationType<ApplicationType>

Gets applications that match the type specified: HostedOnDesktop or InstalledOnClient.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedDesktopGroupPriority<Int32>

Gets applications with an associated desktop group identified by priority assigned to the pairing between an application and desktop group.

Associated desktop group is a desktop group on which the application is published.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedDesktopGroupUid<Int32>

Gets applications with an associated desktop group identified by the desktop group UID.

Associated desktop group is a desktop group on which the application is published.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedDesktopGroupUUID<Guid>

Gets applications with an associated desktop group identified by the desktop group UUID.

Associated desktop group is a desktop group on which the application is published.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserFullName<String>

Gets applications with an associated user identified by their full name (usually 'first-name last-name').

If the 'UserFilterEnabled' property is true then access to the application is restricted to those users only, otherwise access is unrestricted (but always subject to other policy rules).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserName<String>

Gets applications with an associated user identified by their user name (in the form 'domain\user'). If the 'UserFilterEnabled' property is true then access to the application is restricted to those users only, otherwise access is unrestricted (but always subject to other policy rules).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserUPN<String>

Gets applications with an associated user identified by their user principle name (in the form 'user@domain'). If the 'UserFilterEnabled' property is true then access to the application is restricted to those users only, otherwise access is unrestricted (but always subject to other policy rules).

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrowserName<String>

Gets only the applications that match the supplied name. The BrowserName is usually an internal name for the application and is unique in the site.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientFolder<String>

Gets only the applications that match the specified value for the folder the application belongs to as seen by the end-user. This folder can be seen in the Citrix Online Plug-in, in Web Services, and also potentially in the user's start menu.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CommandLineArguments<String>

Gets only the applications that match the supplied arguments to the command-line executable.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CommandLineExecutable<String>

Gets only the applications that match the supplied command-line executable.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CpuPriorityLevel<CpuPriorityLevel>

Gets only the applications that have the specified value for the CPU priority level of the launched executable. Valid values are: Low, BelowNormal, Normal, AboveNormal, and High.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets only the applications that match the supplied description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets only the applications that have the specified value for whether the application is enabled. Disabled applications are still visible to users (that is controlled by the Visible setting) but cannot be launched.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconFromClient<Boolean>

Gets only the applications that have the specified value for whether the application icon should be retrieved from the user device.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Gets only the applications that use the specified icon (identified by its Uid).

Required?	false
Default Value	
Accept Pipeline Input?	false

-MetadataKey<String>

Gets only applications whose associated metadata contains key names matching the specified value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Gets applications whose published name matches the supplied pattern.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureCmdLineArgumentsEnabled<Boolean>

Gets only the applications that have the specified value for whether the command-line arguments should be secured. This is reserved for possible future use, and all applications of type HostedOnDesktop can only have this value set to true.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ShortcutAddedToDesktop<Boolean>

Gets only the applications that match depending on whether a shortcut for the application has been added to the user device or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ShortcutAddedToStartMenu<Boolean>

Gets only the applications that match depending on whether a shortcut for the application has been added to Start Menu of the user device or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartMenuFolder<String>

Gets only the applications that match the specified name for the start menu folder that holds the application shortcut. This is valid only for the Citrix Online Plug-in.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserFilterEnabled<Boolean>

Gets only applications whose user filter is in the specified state.

Required?	false
Default Value	

Accept Pipeline Input?	false

-UUID<Guid>

Gets applications with the specified value of UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Visible<Boolean>

Gets only the applications that have the specified value for whether it is visible to the users.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WaitForPrinterCreation<Boolean>

Gets only the applications that match depending on whether the VDA delays starting the application until printers are set up.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WorkingDirectory<String>

Gets only the applications that match the specified working directory.

Required?	false
Default Value	

Accept Pipeline Input?	false

-DesktopUid<Int32>

Gets only the applications that have been associated (using a desktop group) to the specified desktop (identified by its Uid). Note that an application is not directly associated with a desktop, but only indirectly by which desktop group it has been published to.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUid<Int64>

Gets only the applications that are running in the specified session (identified by its Uid).

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserSID<String>

Gets only applications with their accessibility restricted to include the specified user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets only the applications that have been published to the specified desktop group (identified by its Uid).

Required?	false
Default Value	

Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false

Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Application

Get-BrokerApplication returns an object for each application it gets.

Notes

Get-BrokerApplication returns just the application object, and as such is not a complete picture. The returned objects do not tell you what File-Type Associations are configured for this application, etc.

Use the following cmdlets to gather data related to applications (shown with examples of syntax):

Get-BrokerConfiguredFTA -ApplicationUid $app.Uid

Get-BrokerTag -ApplicationUid $app.Uid

Get-BrokerDesktopGroup -ApplicationUid $app.Uid

Get-BrokerDesktop -PublishedApplication $app

Get-BrokerSession -ApplicationUid $app.Uid

Get-BrokerApplicationInstance -ApplicationUid $app.Uid

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerApplication Notepad
Returns the application with the Name of "Notepad".

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerApplication -PublishedName Note* -Enabled $true
Returns the applications that have a PublishedName starting with "Note" and that are enabled.

Get-BrokerApplicationInstance

Sep 10, 2014

Gets the running applications on the desktops.

Syntax

```
Get-BrokerApplicationInstance -Uid <Int64> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerApplicationInstance [-ApplicationName <String>] [-ApplicationUid <Int32>] [-ApplicationUUID <Guid>] [-Instances <Int32>] [-MachineName <String>] [-MachineUid <Int32>] [-Metadata <String>] [-SessionKey <Guid>] [-SessionUid <Int64>] [-UserName <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Get-BrokerApplicationInstance gets the published applications that are running on desktops.

Only published applications that are launched from a Citrix client are returned. If a user launches an application from within a session (by double-clicking on an attachment from an email, for example) this will not show up in the list of running applications.

Also note that this is a list of launched published applications, not a list of processes running on the desktop. In some cases the original process associated with the published application may no longer be running, but if the session is still running the published application may be listed as running.

The number of instances for each published application running in a session is also returned. For example, if a user launches two Notepad applications from a Citrix client, and session-sharing occurs such that both Notepad applications run in the same session, then the Instances property indicates that 2 copies are running in the session.

See Get-BrokerApplication and Get-BrokerSession to get the details for the applications and sessions, respectively.

The Get-BrokerMachine cmdlet also returns a list of published applications that are running on a desktop. See the "ApplicationsInUse" attribute of the returned desktop objects.

---------- BrokerApplicationInstance Object

The BrokerApplicationInstance object represents an instance of a published application in the site. It contains the following properties:

-- ApplicationName (System.String)

The administrative name of the application.

-- ApplicationUid (System.Int32)

The UID of the application.

-- ApplicationUUID (System.Guid)

The UUID of the application.

-- Instances (System.Int32)

The number of times this published application is running in the specified session.

-- MachineName (System.String)

Machine's SAM name (of the form domain\machine). If SAM name is unavailable, contains the machines's SID.

-- MachineUid (System.Int32)

UID of underlying machine.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Metadata for this application instance.

-- SessionKey (System.Guid)

The key of the session.

-- SessionUid (System.Int64)

The UID of the session.

-- Uid (System.Int64)

The unique identifier for this application instance object itself, distinct from the Uids of either application or session. objects.

-- UserName (System.String)

User name (SAMName).

Related topics

Get-BrokerApplication

Get-BrokerDesktop

Get-BrokerSession

Parameters

-Uid<Int64>

Gets only the application instances specified by the unique identifier. This is the unique identifier for the application instance object itself, and is distinct from the Uids of either application or session objects.

Required?	true
Default Value	

Accept Pipeline Input?	false

-ApplicationName<String>

Gets only application instances for the specified application name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationUid<Int32>

Gets only application instances for the specified application Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationUUID<Guid>

Gets only the application instances for the specified application UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Instances<Int32>

Gets only application instances that match the specified number of instances.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets only application instances running on the specified machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineUid<Int32>

Gets only application instances running on the machine with the specified UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionKey<Guid>

Gets only application instances for the published applications running in the specified session.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUid<Int64>

Gets only application instances for the published applications running in the specified session.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserName<String>

Gets only application instances being run by the specified users.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.ApplicationInstance

Get-BrokerApplicationInstance returns an object for each application instance it gets.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerApplicationInstance -Uid 3
```

Returns the application instance with a Uid of 3. Note that this is the unique identifier for application instances, which is distinct from the unique identifiers of either application or session objects.

---------- EXAMPLE 2 ----------

```
C:\PS> $app = Get-BrokerApplication Notepad
C:\PS> Get-BrokerApplicationInstance -ApplicationUid $app.Uid
```

Returns all the application instances for the Notepad application. Use this to see if there are any launched instances of Notepad running in your site and, if so, from which desktops.

---------- EXAMPLE 3 ----------

```
C:\PS> $sessions = Get-BrokerSession -MachineName "ACME\Worker1"
C:\PS> for ($i=0; $i -lt $sessions.Length; $i++) {
          Get-BrokerApplicationInstance -SessionUid $sessions[$i].SessionUid
        }
```

Returns all the applications that are running on the "Worker1" machine in the "ACME" domain. Use this to see which published applications are running on a specific machine.

Note that the SessionUid, not the SessionId, is specified as a parameter to this cmdlet. The SessionId is a unique identifier that Remote Desktop Services uses to track the session, and is unique only on that machine. The SessionUid, on the other

hand, is unique across the entire site.

The "ApplicationsInUse" attribute of the returned session object also provides a list of running launched applications, and in many cases might be more convenient to use. It returns a list of application BrowserNames.

Get-BrokerAssignmentPolicyRule

Sep 10, 2014

Gets desktop rules from the site's assignment policy.

Syntax

```
Get-BrokerAssignmentPolicyRule [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerAssignmentPolicyRule [[-Name] <String>] [-ColorDepth <ColorDepth>] [-Description <String>] [-DesktopGroupUid <Int32>] [-Enabled <Boolean>] [-ExcludedUser <User>] [-ExcludedUserFilterEnabled <Boolean>] [-IconUid <Int32>] [-IncludedUser <User>] [-IncludedUserFilterEnabled <Boolean>] [-MaxDesktops <Int32>] [-Metadata <String>] [-PublishedName <String>] [-SecureIcaRequired <Boolean>] [-UUID <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns desktop rules matching the specified search criteria from the site's assignment policy. If no search criteria are specified, all desktop rules in the assignment policy are obtained.

A desktop rule in the assignment policy defines the users who are entitled to self-service persistent machine assignments from the rule's desktop group. A rule defines how many machines a user is allowed from the group for delivery of full desktop sessions.

---------- BrokerAssignmentPolicyRule Object

The BrokerAssignmentPolicyRule object represents a single desktop rule within the site's assignment policy. It contains the following properties:

-- ColorDepth (Citrix.Broker.Admin.SDK.ColorDepth?)

The color depth of desktop sessions launched by the user from machines assigned to them by the rule. If null, the equivalent setting from the rule's desktop group is used.

-- Description (System.String)

Optional description of the rule. The text may be visible to the end user, for example, as a tooltip associated with the desktop entitlement.

-- DesktopGroupUid (System.Int32)

The unique ID of the desktop group to which the rule applies.

-- Enabled (System.Boolean)

Indicates whether the rule is enabled. A disabled rule is ignored when evaluating the site's assignment policy.

-- ExcludedUserFilterEnabled (System.Boolean)

Indicates whether the excluded users filter is enabled. If the filter is disabled then any user entries in the filter are ignored when assignment policy rules are evaluated.

-- ExcludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

The excluded users filter of the rule, that is, the users and groups who are explicitly denied entitlements to machine assignments from the rule's desktop group.

-- IconUid (System.Int32?)

The unique ID of the icon used for the machine entitlement seen by the user or, after a machine is assigned by the rule, the icon for the desktop itself. If null, the equivalent setting from the rule's desktop group is used.

-- IncludedUserFilterEnabled (System.Boolean)

Indicates whether the included users filter is enabled. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly entitled to the machine assignments described by the rule.

For rules that relate to RemotePC desktop groups however, if the included user filter is disabled, the rule is effectively disabled.

-- IncludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

The included users filter of the rule, that is, the users and groups who are entitled to machine assignments from the rule's desktop group.

-- MaxDesktops (System.Int32)

The number of machines from the rule's desktop group to which a user is entitled. Where an entitlement is granted to a user group rather than an individual, the number of machines applies to each member of the user group independently.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

A collection of arbitrary key/value pairs that can be associated with the rule. The administrator can use these values for any purpose; they are not used by the site itself in any way.

-- Name (System.String)

The administrative name of the rule. Each rule in the site's assignment policy must have a unique name (irrespective of whether they are desktop or application rules).

-- PublishedName (System.String)

The published name of the desktop entitlement seen by the user or, after a machine is assigned by the rule, the published name of the desktop itself. If null, the equivalent setting from the rule's desktop group is used.

-- SecureIcaRequired (System.Boolean?)

Indicates whether the rule requires the SecureICA protocol for desktop sessions launched using a machine assigned by the rule. If null, the equivalent setting from the rule's desktop group is used.

-- Uid (System.Int32)

The unique ID of the rule itself.

-- UUID (System.Guid)

UUID of the rule.

Related topics

New-BrokerAssignmentPolicyRule

Set-BrokerAssignmentPolicyRule

Rename-BrokerAssignmentPolicyRule

Remove-BrokerAssignmentPolicyRule

Parameters

-Uid<Int32>

Gets the desktop rule with the specified unique ID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets only desktop rules with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Gets only desktop rules with the specified color depth.

Valid values are $null, FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets only desktop rules with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets only desktop rules that apply to the desktop group with the specified unique ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets only rules that are in the specified state, either enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUser<User>

Gets only desktop rules that have the specified user in their excluded users filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Gets only desktop rules that have their excluded user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Gets only desktop rules using the icon with the specified unique ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUser<User>

Gets only desktop rules that have the specified user in their included users filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Gets only desktop rules that have their included user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxDesktops<Int32>

Gets only desktop rules granting the specified number of machine assignment entitlements.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Gets only desktop rules with the specified published name, that is, the desktop name that the end user sees.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Gets only desktop rules that require desktop sessions to machines assigned by the rule to use the SecureICA protocol ($true) or not ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-UUID<Guid>

Gets rules with the specified value of UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.

Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.AssignmentPolicyRule

Get-BrokerAssignmentPolicyRule returns all assignment policy rules that match the specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerAssignmentPolicyRule
```

Returns all desktop rules from the assignment policy. This offers a complete description of the current site's assignment policy with respect to machine assignment entitlements for delivery of desktop sessions from private desktop groups.

---------- EXAMPLE 2 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Sales Support'
C:\PS> Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid
```

Returns all rules in the assignment policy that give users entitlements to machine assignments in the Sales Support desktop group for delivery of full desktop sessions.

Get-BrokerCatalog

Jan 19, 2017

Gets catalogs configured for this site.

Syntax

Get-BrokerCatalog [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerCatalog [[-Name] <String>] [-AllocationType <AllocationType>] [-AssignedCount <Int32>] [-AvailableAssignedCount <Int32>] [-AvailableCount <Int32>] [-AvailableUnassignedCount <Int32>] [-Description <String>] [-HypervisorConnectionUid <Int32>] [-IsRemotePC <Boolean>] [-MachinesArePhysical <Boolean>] [-Metadata <String>] [-MinimumFunctionalLevel <FunctionalLevel>] [-PersistUserChanges <PersistUserChanges>] [-ProvisioningSchemeId <Guid>] [-ProvisioningType <ProvisioningType>] [-PvsAddress <String>] [-PvsDomain <String>] [-RemotePCDesktopGroupPriority <Int32>] [-RemotePCDesktopGroupUid <Int32>] [-RemotePCHypervisorConnectionUid <Int32>] [-ScopeId <Guid>] [-ScopeName <String>] [-SessionSupport <SessionSupport>] [-UnassignedCount <Int32>] [-UsedCount <Int32>] [-UUID <Guid>] [-MachineUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieves catalogs matching the specified criteria. If no parameters are specified this cmdlet enumerates all catalogs.

See about_Broker_Filtering for information about advanced filtering options.

---------- BrokerCatalog Object

The catalog object returned represents a group of related physical or virtual machines that have been configured in the site.

See about_Broker_Machines for more information.

-- AllocationType (Citrix.Broker.Admin.SDK.AllocationType)

Denotes how the the machines in the catalog are allocated to a user.

Possible values are:

o Static: Machines get assigned to a user either by the admin or on first use. This relationship is static and changes only if an admin explicitly changes the assignments. o Random: Machines are allocated to users randomly from a pool of available machines.

-- AssignedCount (System.Int32)

The number of assigned machines (machines that have been assigned to a user/users or a client name/address).

-- AvailableAssignedCount (System.Int32)

The number of available machines (not in a desktop group), that are also assigned to users.

-- AvailableCount (System.Int32)

The number of available machines (those not in any desktop group).

-- AvailableUnassignedCount (System.Int32)

The number of available machines (those not in any desktop group) that are not assigned to users.

-- Description (System.String)

Description of the catalog.

-- HypervisorConnectionUid (System.Int32?)

The Uid of the hypervisor connection that is associated with the machines in the catalog. This property only applies to MCS provisioned catalogs. For other provisioning types machines can be from one or more different hypervisor connections.

-- IsRemotePC (System.Boolean)

Specifies whether or not the catalog is a RemotePC catalog. Remote PC catalogs automatically configure appropriate machines without the need for manual configuration. See about_Broker_RemotePC for more information.

-- MachinesArePhysical (System.Boolean)

Specifies whether or not the machines in the catalog can be power-managed by the broker.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Holds any metadata associated with the catalog.

-- MinimumFunctionalLevel (Citrix.Broker.Admin.SDK.FunctionalLevel)

The expected minimal functional level of the machines in the catalog.

-- Name (System.String)

Name of the catalog.

-- PersistUserChanges (Citrix.Broker.Admin.SDK.PersistUserChanges)

Specifies how user changes are persisted on machines in the catalog. Possible values are:

o OnLocal: User changes are stored on the machine's local storage.

o Discard: User changes are discarded.

o OnPvd: User changes are stored on the user's personal vDisk.

-- ProvisioningSchemeId (System.Guid?)

The GUID of the provisioning scheme (if any) associated with the catalog. This only applies if the provisioning type is MCS.

-- ProvisioningType (Citrix.Broker.Admin.SDK.ProvisioningType)

Specifies how the machines are provisioned in the catalog. Possible values are:

o Manual: No provisioning.

o PVS: Machine provisioned by PVS (machine may be physical, blade, VM...)

o MCS: Machine provisioned by MCS (machine must be a VM).

-- PvsAddress (System.String)

IP address of the PVS server to be used in a catalog with a PVS ProvisioningType.

-- PvsDomain (System.String)

The domain of the PVS server to be used in a catalog with a PVS ProvisioningType.

-- RemotePCDesktopGroupPriorities (System.Int32[])

Remote PC desktop groups' association priorities.

-- RemotePCDesktopGroupUids (System.Int32[])

UIDs of the Remote PC desktop groups associated with this catalog.

-- RemotePCHypervisorConnectionUid (System.Int32?)

UID of the hypervisor connection used for powering on RemotePC machines in this catalog (only for catalogs with IsRemotePC set to true).

-- Scopes (Citrix.Broker.Admin.SDK.ScopeReference[])

The list of the delegated admin scopes to which the catalog belongs.

-- SessionSupport (Citrix.Broker.Admin.SDK.SessionSupport)

Specifies the session support of the machines in the catalog. Valid values are:

SingleSession, MultiSession.

-- Uid (System.Int32)

Uid of the catalog.

-- UnassignedCount (System.Int32)

The number of unassigned machines (machines not assigned to users).

-- UsedCount (System.Int32)

An array of machines in the catalog that are in a desktop group.

-- UUID (System.Guid)

The global ID of the catalog.

Related topics

New-BrokerCatalog

Remove-BrokerCatalog

Rename-BrokerCatalog

Set-BrokerCatalog

Parameters

-Uid<Int32>

Get catalogs with the specified UID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets catalogs with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AllocationType<AllocationType>

Gets catalogs that are of the specified allocation type. Values can be:

o Static - Machines in a catalog of this type are permanently assigned to a user.

o Permanent - equivalent to 'Static'.

o Random - Machines in a catalog of this type are picked at random and temporarily assigned to a user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedCount<Int32>

Gets catalogs containing a specified number of assigned machines (machines that have been assigned to users).

This property is typically used with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AvailableAssignedCount<Int32>

Gets catalogs containing a specified number of available machines (those not in any desktop group) that are also assigned to users.

This property is typically used with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AvailableCount<Int32>

Gets catalogs containing a specified number of available machines (those not in any desktop group).

This property is typically used with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AvailableUnassignedCount<Int32>

Gets catalogs containing a specified number of available machines (those not in any desktop group) that are not assigned to users.

This property is typically used with advanced filtering; see about_Broker_Filtering.

Required?	false

Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets catalogs with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets catalogs associated with the specified hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsRemotePC<Boolean>

Gets catalogs with the specified IsRemotePC value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachinesArePhysical<Boolean>

Specifies whether machines in the catalog can be power-managed by the Citrix Broker Service. Where the Citrix Broker Service cannot control the power state of the machine specify $true, otherwise $false. Can only be specified together with a provisioning type of Pvs or Manual, or if used with the legacy CatalogKind parameter only with Pvs or PvsPvd catalog kinds.

Required?	false

Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-MinimumFunctionalLevel<FunctionalLevel>

Gets catalogs with a specific MinimumFunctionalLevel.

Valid values are L5, L7, L7_6

Required?	false
Default Value	
Accept Pipeline Input?	false

-PersistUserChanges<PersistUserChanges>

Gets catalogs with the specified behavior when persisting changes made by the end user. Possible values are:

o OnLocal - User changes are stored on the machine's local storage.

o Discard - User changes are discarded.

o OnPvd - User changes are stored on the user's personal vDisk.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ProvisioningSchemeId<Guid>

Gets catalogs associated with the specified provisioning scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningType<ProvisioningType>

Specifies the provisioning type for the catalog. Values can be:

o Manual - No provisioning.

o PVS - Machine provisioned by PVS (machine may be physical, blade, VM,...).

o MCS - Machine provisioned by MCS (machine must be VM).

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvsAddress<String>

Gets catalogs containing machines provided by the Provisioning Services server with the specified address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvsDomain<String>

Gets catalogs containing machines provided by the Provisioning Services server in the specified domain.

Required?	false

Default Value	
Accept Pipeline Input?	false

-RemotePCDesktopGroupPriority<Int32>

Gets Remote PC catalogs with a Remote PC desktop group association with the specified priority.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemotePCDesktopGroupUid<Int32>

Gets Remote PC catalogs associated with the specified Remote PC desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemotePCHypervisorConnectionUid<Int32>

Gets Remote PC catalogs associated with the specified Remote PC hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScopeId<Guid>

Gets catalogs that are associated with the given scope identifier.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ScopeName<String>

Gets catalogs that are associated with the given scope name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSupport<SessionSupport>

Gets catalogs that have the specified session capability. Values can be:

o SingleSession - Single-session only machine.

o MultiSession - Multi-session capable machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UnassignedCount<Int32>

Gets catalogs containing a specified number of unassigned machines (machines not assigned to users).

This property is typically used with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UsedCount<Int32>

Gets catalogs containing a specified number of machines used in a desktop group.

This property is typically used with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UUID<Guid>

Get catalogs with the specified global ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineUid<Int32>

Gets the catalog containing the machine referenced by the specified unique identifier (UID).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None

Return Values

Citrix.Broker.Admin.SDK.Catalog

Get-BrokerCatalog returns an object for each matching catalog.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerCatalog -AllocationType Random
C:\PS> Get-BrokerCatalog -Filter { AllocationType  -eq 'Random'}
```

These commands return all catalogs containing machines that are randomly assigned to users. The second form uses advanced filtering (see about_Broker_Filtering).

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerCatalog -Filter { AvailableCount  -gt 10}
```

This command returns catalogs with more than 10 unused machines that are available for assignment to users.

---------- EXAMPLE 3 ----------

```
C:\PS> Get-BrokerCatalog -MaxRecordCount 1 -ProvisioningType Manual -SortBy '-AvailableCount'
```

This command returns the unmanaged catalog with the highest number of available machines.

Get-BrokerConfigurationSlot

Sep 10, 2014

Gets configuration slots configured for this site.

Syntax

```
Get-BrokerConfigurationSlot [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Get-BrokerConfigurationSlot [[-Name] <String>] [-Metadata <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Get the list of configuration slots defined for this site. Each configuration slot determines a collection of related settings that can be specified in a machine configuration associated with this slot.

For example, a configuration slot may be defined to configure only "User Profile Manager" settings.

See about_Broker_Filtering for information about advanced filtering options.

---------- BrokerConfigurationSlot Object

The configuration slot object returned represents a named collection of related settings.

-- Description (System.String)

Optional description of this configuration slot.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

A map of metadata associated with this configuration slot.

-- Name (System.String)

Unique name of this configuration slot.

-- SettingsGroup (System.String)

The encoded identity of the settings group that every setting in the associated machine configuration instances must belong to.

-- Uid (System.Int32)

Unique Uid of this configuration slot.

Related topics

New-BrokerConfigurationSlot

Remove-BrokerConfigurationSlot

Parameters

-Uid<Int32>

Get only the configuration slot with the specified unique identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Get only the configuration slot with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false

Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.ConfigurationSlot

Get-BrokerConfigurationSlot returns an object for each matching slot.

Examples

---------- EXAMPLE 1 ----------

Get-ConfigurationSlot
Retrieves every configuration slot.

---------- EXAMPLE 2 ----------

```
Get-ConfigurationSlot -Name "AppV"
```

Retrieves the configuration slot named "AppV".

Get-BrokerConfiguredFTA

Sep 10, 2014

Gets any file type associations configured for an application.

Syntax

```
Get-BrokerConfiguredFTA -Uid <Int32> [-Property <String[]>] [-AdminAddress <String>]
[<CommonParameters>]

Get-BrokerConfiguredFTA [-ApplicationUid <Int32>] [-ContentType <String>] [-ExtensionName <String>]
[-HandlerDescription <String>] [-HandlerName <String>] [-HandlerOpenArguments <String>] [-UUID
<Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-
Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets any file type associations that are configured for content redirection to a published application.

File type association associates a file extension (such as ".txt") with an application (such as Notepad). In a Citrix environment file type associations on a user device can be configured so that when an user clicks on a document it launches the appropriate published application. This is known as "content redirection".

Configured file type associations are different from imported file type associations. Configured file type associations are those that are actually associated with published applications for the purposes of content redirection. Imported file type associations are lists of known file type associations for a given desktop group. See Update-BrokerImportedFTA for more information about imported file type associations.

---------- BrokerConfiguredFTA Object

The BrokerConfiguredFTA object represents a file type association configured for a published application. It contains the following properties:

-- ApplicationUid (System.Int32)

The Uid of the application configured for the file type association.

-- ContentType (System.String)

Content type of the file, such as "text/plain" or "application/vnd.ms-excel".

-- ExtensionName (System.String)

A single file extension, such as .txt, unique within the scope of a desktop group.

-- HandlerDescription (System.String)

File type description, such as "Test Document", "Microsoft Word Text Document", etc.

-- HandlerName (System.String)

File type handler name, e.g. "Word.Document.8" or TXTFILE.

-- HandlerOpenArguments (System.String)

The arguments used for the 'open' action on files of this type.

-- Uid (System.Int32)

Unique internal identifier of configured file type association.

-- UUID (System.Guid)

UUID of the configured file type association.

Related topics

New-BrokerConfiguredFTA

Remove-BrokerConfiguredFTA

Update-BrokerImportedFTA

Parameters

-Uid<Int32>

Gets only the configured file type association for the specified unique identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ApplicationUid<Int32>

Gets only the configured file type associations for the specified application unique identifier.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ContentType<String>

Gets only the configured file type associations for the specified content type (as seen in the Registry). For example, "text/plain" or "application/msword".

Required?	false

Default Value	
Accept Pipeline Input?	false

-ExtensionName<String>

Gets only the configured file type associations for the specified extension name. For example, ".txt" or ".doc".

Required?	false
Default Value	
Accept Pipeline Input?	false

-HandlerDescription<String>

Gets only the configured file type associations for the specified handler description. For example, "Text Document".

Required?	false
Default Value	
Accept Pipeline Input?	false

-HandlerName<String>

Gets only the configured file type associations for the specified handler name. For example, "TXTFILE" or "Word.Document.8".

Required?	false
Default Value	
Accept Pipeline Input?	false

-HandlerOpenArguments<String>

Gets only the configured file type associations for the specified open argument to the handler. For example, "%1".

Required?	false

Default Value	
Accept Pipeline Input?	false

-UUID<Guid>

Gets configured file type associations with the specified value of UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false

Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None No input is accepted from the pipeline.

Return Values

Citrix.Broker.Admin.SDK.ConfiguredFTA

This cmdlet returns one or more ConfiguredFTA objects.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerConfiguredFTA
Returns all configured file type associations.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerConfiguredFTA -ExtensionName ".txt"
Returns only configured file type associations that have a ".txt" extension.

Get-BrokerConnectionLog

Sep 10, 2014

Get entries from the site's session connection log.

Syntax

Get-BrokerConnectionLog [-Uid] <Int64> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerConnectionLog [[-MachineName] <String>] [-BrokeringTime <DateTime>] [-BrokeringUserName <String>] [-BrokeringUserUPN <String>] [-ConnectionFailureReason <ConnectionFailureReason>] [-Disconnected <Boolean>] [-EndTime <DateTime>] [-EstablishmentTime <DateTime>] [-MachineDNSName <String>] [-MachineUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets connection log entries matching the specified criteria. If no parameters are specified all connection log entries are returned.

The session connection log contains entries describing each brokered connection, or reconnection, attempt to a session in the site.

Each log entry describes a single connection brokering attempt to a new or existing session within the site. A single session can have multiple entries in the connection log, for example where the end user brokers a connection to a new session, disconnects and later brokers a reconnection. Conversely, other sessions may have none (e.g. console sessions).

By default connection log entries are removed after 48 hours.

For information about advanced filtering options when using the -Filter parameter, see about_Broker_Filtering; for information about machines, see about_Broker_Machines.

---------- BrokerConnectionLog Object

The BrokerConnectionLog object represents a single brokered connection attempt to a new or existing session on a machine in the site. It contains the following properties:

-- BrokeringTime (System.DateTime)

The time at which the connection attempt was made.

-- BrokeringUserName (System.String)

The name of the user making the connection (in DOMAIN\User format).

-- BrokeringUserUPN (System.String)

The name of the user making the connection (in user@upndomain.com format).

-- ConnectionFailureReason (Citrix.Broker.Admin.SDK.ConnectionFailureReason?)

The status of the connection attempt. A value of None indicates that the connection was successfully established, $null that the attempt is still in progress, and other values indicate that the attempt failed for the specified reason.

-- Disconnected (System.Boolean?)

Indicates if the connection was ended by disconnection (True), logoff or establishment failure (False), or is still active ($null).

-- EndTime (System.DateTime?)

The time at which the connection ended. If the connection ended by disconnection, the underlying machine session would still exist in a disconnected state.

-- EstablishmentTime (System.DateTime?)

The time at which the connection was successfully established. The value is $null if the connection attempt failed or is still in progress.

-- MachineDNSName (System.String)

The name of the machine to which the connection was made (in machine@dnsdomain.com form).

-- MachineName (System.String)

The name of the machine to which the connection was made (in DOMAIN\Machine format).

-- MachineUid (System.Int32)

The UID of the machine to which the connection was made.

-- Uid (System.Int64)

The UID of the connection log entry itself.

Related topics

Parameters

-Uid<Int64>

Gets a specific connection log entry identified by its UID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets connection log entries for the specified machines (in DOMAIN\Machine format).

Required?	false

Default Value	
Accept Pipeline Input?	false

-BrokeringTime<DateTime>

Gets connection log entries with a specified brokering time. For more flexibility when searching on brokering time use the -Filter parameter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringUserName<String>

Gets connection log entries for the specified users (in DOMAIN\User format).

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringUserUPN<String>

Gets connection log entries for the specified users (in user@upndomain.com format).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectionFailureReason<ConnectionFailureReason>

Gets connection log entries which failed for the specified reason.

Required?	false

Default Value	
Accept Pipeline Input?	false

-Disconnected<Boolean>

Gets connection log entries with the specified disconnection status, that is, whether the connection was disconnected, or logged-off.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EndTime<DateTime>

Gets connection log entries with the specified end time. For more flexibility when searching on end time use the -Filter parameter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EstablishmentTime<DateTime>

Gets connection log entries with the specific establishment time. For more flexibility when searching on establishment time use the -Filter parameter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineDNSName<String>

Gets connection log entries for the specified machines (in machine@dnsdomain.com format).

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineUid<Int32>

Gets connection log entries for a specific machine identified by its UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.ConnectionLog

An entry from the connection log.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $when = [DateTime]::Now - [TimeSpan]::FromMinutes(30)
C:\PS> Get-BrokerConnectionLog -Filter {BrokeringTime -gt $when} -SortBy '+MachineName,-EndTime'
```

Gets all connection log entries for sessions brokered in the past 30 minutes, ordered first by machine name (ascending), then by session end time (descending).

Get-BrokerController

Sep 10, 2014

Gets Controllers running broker services in the site.

Syntax

```
Get-BrokerController [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>]
[<CommonParameters>]

Get-BrokerController [[-MachineName] <String>] [-ControllerVersion <String>] [-DesktopsRegistered
<Int32>] [-DNSName <String>] [-LastActivityTime <DateTime>] [-LastLicensingServerEvent
<LicensingServerEvent>] [-LastLicensingServerEventTime <DateTime>] [-LastStartTime <DateTime>] [-
LicensingGraceState <LicensingGraceState>] [-LicensingServerState <LicensingServerState>] [-
Metadata <String>] [-OSType <String>] [-OSVersion <String>] [-SID <String>] [-State <ControllerState>]
[-UUID <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>]
[-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets Controllers from the current site that match the specified search criteria.

Controllers are server machines running instances of the broker service. The broker service is responsible for the brokering of user sessions to desktops or applications, and for power management of the underlying machines. An operational site must contain at least one Controller.

If no search criteria are specified, all Controllers in the site are obtained.

---------- BrokerController Object

The BrokerController object represents a single controller running an instance of the Broker service. It contains the following properties:

-- ActiveSiteServices (System.String[])

The Broker site services active on the controller.

-- AssociatedHypervisorConnectionUids (System.Int32[])

The UIDs of the hypervisor connections being managed by the Broker service on the controller.

-- ControllerVersion (System.String)

The version of the Broker service on the controller.

-- DesktopsRegistered (System.Int32)

The number of VDA machines registered with the Broker service on the controller.

-- DNSName (System.String)

The DNS name of the controller.

-- LastActivityTime (System.DateTime?)

The last reported activity time of the Broker service on the controller.

-- LastLicensingServerEvent (Citrix.Broker.Admin.SDK.LicensingServerEvent?)

Last significant licensing server event reported by the Broker service on the controller.

-- LastLicensingServerEventDetails (System.String[])

Additional details associated with the last significant licensing server event.

-- LastLicensingServerEventTime (System.DateTime?)

Time at which the last significant licensing server event was reported.

-- LastStartTime (System.DateTime?)

The last start-up time of the Broker service on the controller.

-- LicensingGracePeriodReasons (Citrix.Broker.Admin.SDK.LicensingGracePeriodReason[])

Current active or expired licensing grace periods in effect on the controller.

-- LicensingGracePeriodTimesRemaining (System.TimeSpan[])

Times remaining in currently active or expired licensing grace periods in effect on the controller. Expired grace periods are indicated by zero remaining time. The number and order of entries in this list matches that in the LicensingGracePeriodReasons list.

-- LicensingGraceState (Citrix.Broker.Admin.SDK.LicensingGraceState)

The licensing grace state currently in effect in the Broker service on the controller.

-- LicensingServerState (Citrix.Broker.Admin.SDK.LicensingServerState)

The licensing server state currently in effect in the Broker service on the controller.

-- MachineName (System.String)

The Windows name of the controller.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

The metadata for the controller.

-- OSType (System.String)

The Operating System type of the controller.

-- OSVersion (System.String)

The Operating System version of the controller.

-- SID (System.String)

The SID of the controller.

-- State (Citrix.Broker.Admin.SDK.ControllerState)

The state of the Broker service on the controller.

-- Uid (System.Int32)

The UID of the controller instance.

-- UUID (System.Guid)

A globally unique identifier of the controller instance.

Related topics

Get-BrokerDesktop

Parameters

-Uid<Int32>

Gets only Controller with the specified unique ID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets only Controllers with the specified Windows name. ('domain\machine')

Required?	false
Default Value	
Accept Pipeline Input?	false

-ControllerVersion<String>

Gets only Controllers running the specified version of the broker service.

Required?	false
Default Value	

Accept Pipeline Input?	false

-DesktopsRegistered<Int32>

Gets only Controllers that have the specified number of desktops currently registered. This parameter is mainly of use with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets only Controllers with the specified DNS name ('machine.domain')

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastActivityTime<DateTime>

Gets only Controllers last reported as active at the specified time. This parameter is mainly of use with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastLicensingServerEvent<LicensingServerEvent>

Gets only Controllers with the specified last license server event recorded.

Required?	false
Default Value	

Accept Pipeline Input?	false

-LastLicensingServerEventTime<DateTime>

Gets only Controllers with its last recorded licensing server event at the specified time. This parameter is mainly of use with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastStartTime<DateTime>

Gets only Controllers that last started-up at the specified time. This parameter is mainly of use with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LicensingGraceState<LicensingGraceState>

Gets only Controllers in the specified licensing grace state.

Valid values are: NotActive, InOutOfBoxGracePeriod, InSupplementalGracePeriod, InEmergencyGracePeriod and GracePeriodExpired.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LicensingServerState<LicensingServerState>

Gets only Controllers in the specified licensing server state. Valid values are: ServerNotSpecified, NotConnected, OK, LicenseNotInstalled, LicenseExpired, Incompatible and Failed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets only Controllers running the specified Operating System type.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSVersion<String>

Gets only Controllers running the specified Operating System version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SID<String>

Gets only Controllers with the specified SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-State<ControllerState>

Gets only Controllers currently in the specified state.

Valid values are: Failed, Off, On, and Active.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UUID<Guid>

Gets only the Controller with the specified GUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Controller

Returns Controllers matching all specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerController -State Active
```

Gets all Controllers in the site that are currently active (powered on and fully operational).

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerController -Filter 'LastStartTime -gt "-30:00"'
```

Gets all Controllers in the site that started-up in the last 30 minutes.

Get-BrokerDBConnection

Sep 10, 2014

Gets the database connection string for the specified data store used by the Broker Service.

Syntax

```
Get-BrokerDBConnection [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets the database connection string from the currently selected Broker Service instance.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

The current service instance is the one on the local machine, or the one most recently specified using the -AdminAddress parameter of a Broker SDK cmdlet.

Related topics

Set-BrokerDBConnection

Get-BrokerServiceStatus

Test-BrokerDBConnection

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

System.String

The database connection string configured for the current Broker Service instance.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the Broker Service has not been specified.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerDBConnection -AdminAddress controller1.mydomain.net
```

Gets the database connection string in use by the Broker Service instance running on controller "controller1.mydomain.net".

Get-BrokerDBSchema

Sep 10, 2014

Gets SQL scripts to create or maintain the database schema for the Citrix Broker Service.

Syntax

```
Get-BrokerDBSchema -DatabaseName <String> [-ServiceGroupName <String>] [-ScriptType
<DatabaseScriptType>] [-SID <String>] [-LocalDatabase] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets SQL scripts that can be used to create a new Citrix Broker Service database schema, add a new Broker service to an existing site, remove a Broker service from a site, or create a database server logon for a Broker service.

If no Sid parameter is provided, the scripts obtained relate to the currently selected Broker service instance, otherwise the scripts relate to Broker service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied.

The current service instance is the one on the local machine, or the one most recently specified using the -AdminAddress parameter of a Broker SDK cmdlet.

The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured.

The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SQLCMD mode'.

The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to Broker service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to Broker service roles

If ScriptType is Evict, the returned script contains:

o Removal of Broker service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database.

You do not need to configure a database before using this command.

Related topics

Set-BrokerDBConnection

Test-BrokerDBConnection

Parameters

-DatabaseName<String>

Specifies the name of the database into which the new Broker service schema is to be placed, or in which it already exists. The database itself is not created by any of the script types; it must already exist before the scripts are run.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the Broker services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<DatabaseScriptType>

Specifies the type of database script returned. Available script types are:

-- FullDatabase

Creates a database schema for the Citrix Broker Service in a database instance that does not already contain one. This is used when creating a new site. DatabaseName and ServiceGroupName are required parameters for this script type.

-- Instance

Adds a Broker Service instance to a database and so to the associated site. Appropriate database server logons and users are created to allow the service instance access to the required service schemas.

-- Evict

Removes a Broker Service instance from the database and so from the site. All reference to the service instance is removed from the database. DatabaseName and Sid are required parameters for this script type.

-- Login

Adds a logon for the Broker Service instance to a database server. This is specifically for use when configuring SQL Server mirroring where the mirror server must have appropriate logons created for all service instances in the site.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SID<String>

Specifies the SID of the controller on which the Broker Service instance to remove from the database is running (only valid for a script type of Evict).

Required?	false
Default Value	None
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for Broker services. If this parameter is specified inappropriately, the service instance will not be able to connect to the database.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

System.String

A string containing the required SQL script for applying to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-BrokerDBSchema -DatabaseName MySiteDB -ServiceGroupName  MyServiceGroup > C:\BrokerSchema.sql
```

Gets a script to create the full database schema for the Citrix Broker Service and copies it to a file called "C:\BrokerSchema.sql"

This script can be used to create the service schema in a database with name "MySiteDB", which must already exist, and must not already contain a Broker service schema.

---------- EXAMPLE 2 ----------

```
C:\PS>Get-BrokerDBSchema -DatabaseName MySiteDB -ScriptType Login > C:\BrokerLogins.sql
```

Gets a script to create the appropriate database server logon for the Broker service. This can be used when configuring a mirror server for use.

Get-BrokerDBVersionChangeScript

Sep 10, 2014

Gets an SQL service schema update script for the Citrix Broker Service.

Syntax

```
Get-BrokerDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets an SQL script that can be used to update the current Citrix Broker Service database schema. An update can be an upgrade or downgrade.

A script can be obtained to update the current service schema to any version that is reachable by applying available schema update packages that have been uploaded by the Citrix Broker Service.

Typically, this mechanism is used to update the current service schema to a newer version, however it can also be used to revert previously applied updates.

The SQL script obtained can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SQLCMD mode'.

The schema update packages used to generate update scripts are stored in the database; because of this, any Citrix Broker Service in the site can be used to obtain a schema update script.

The fact that an update package is available in the database does not mean that the update has actually been applied to the service's schema. In addition, application of an update does not remove the associated update packages.

Take care when using the update scripts. Citrix recommends that where possible service schema upgrades are performed using Studio rather than manually via the SDK. The database should be backed-up before an update is attempted. The database script may also require exclusive use of the schema, in which case all Citrix Broker Services must be shutdown before applying the update.

Once an update has been applied to the service schema, any existing Citrix Broker Services that are incompatible with the updated schema will cease to operate. The service state, as reported by Get-BrokerServiceStatus, provides information about the service compatibility (e.g. DBNewerVersionThanService).

Related topics

Get-BrokerInstalledDBVersion

Get-BrokerServiceStatus

Get-BrokerDBSchema

Parameters

-DatabaseName<String>

The name of the database containing the Citrix Broker Service schema to be updated.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

The required target service schema version of the update. This is the service schema version obtained after the update script is applied.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

System.Management.Automation.PSObject

The Get-BrokerDBVersionChangeScript cmdlet returns a PSObject containing a script that can be used to update the Citrix Broker Service database schema. The object has the following properties:

-- Script

The raw text of the SQL script to apply the update.

-- CanUndo

If true, indicates that after the update has been applied, a script to revert from the updated schema to the schema state prior to the update can be obtained. Because Get-BrokerDBVersionChangeScript gets only update scripts relating to the current schema version, a script to revert an update can be obtained only after the update has been applied.

-- NeedExclusiveAccess

If true, indicates that the update requires exclusive access to the Citrix Broker Service's schema while the update is applied; all Citrix Broker Services must be shutdown during the update.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any Broker services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-BrokerServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Broker Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $update = Get-BrokerDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
        C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-BrokerDelayedHostingPowerAction

Sep 10, 2014

Gets power actions that are executed after a delay.

Syntax

```
Get-BrokerDelayedHostingPowerAction [-Uid] <Int64> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerDelayedHostingPowerAction [[-MachineName] <String>] [-Action <PowerManagementAction>] [-ActionDueTime <DateTime>] [-DNSName <String>] [-HostedMachineName <String>] [-HypervisorConnectionName <String>] [-HypervisorConnectionUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Finds all delayed power actions that match the specified search criteria.

---------- BrokerDelayedHostingPowerAction Object

The BrokerDelayedHostingPowerAction object represents an instance of a power action that is executed after a delay. It contains the following properties:

-- Action (Citrix.Broker.Admin.SDK.PowerManagementAction)

The power action to apply to the machine. Possible values are ShutDown and Suspend.

-- ActionDueTime (System.DateTime)

The UTC time at which the power action is due to be queued for execution.

-- DNSName (System.String)

The fully qualified DNS name of the machine that the power action applies to.

-- HostedMachineName (System.String)

The hypervisor's name for the machine that the power action applies to.

-- HypervisorConnectionUid (System.Int32)

The unique identifier of the hypervisor connection that is associated with the target machine.

-- MachineName (System.String)

The name of the machine that the power action applies to, in the form domain\machine.

-- Uid (System.Int64)

The unique identifier of the power action.

Related topics

New-BrokerDelayedHostingPowerAction

Remove-BrokerDelayedHostingPowerAction

Remove-BrokerHostingPowerAction

Parameters

-Uid<Int64>

Gets only the single action record whose ID matches the specified value.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets only the records for actions that are for machines whose name (of the form domain\machine) matches the specified string.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Action<PowerManagementAction>

Gets only the records for actions with the specified action type.

Valid values are Shutdown and Suspend.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ActionDueTime<DateTime>

Gets only the records for actions due to be queued for execution at the specified time. This is useful with advanced filtering; for more information, see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets only the records for actions that are for machines whose DNS name matches the specified string.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets only the records for actions that are for machines whose Hosting Name (the machine name as understood by the hypervisor) matches the specified string.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionName<String>

Gets only the records for actions for machines hosted through a hypervisor connection whose name matches the specified string.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets only the records for actions for machines hosted through a hypervisor connection whose ID matches the specified value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0

Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.DelayedHostingPowerAction

Get-BrokerDelayedHostingPowerAction returns all delayed power actions that match the specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerDelayedHostingPowerAction
Fetches records for all known delayed power actions that have not yet been queued for execution.

Get-BrokerDesktop

Sep 10, 2014

Gets desktops configured for this site.

Syntax

Get-BrokerDesktop [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerDesktop [[-MachineName] <String>] [-AgentVersion <String>] [-ApplicationInUse <String>] [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-AssociatedUserFullName <String>] [-AssociatedUserName <String>] [-AssociatedUserUPN <String>] [-AutonomouslyBrokered <Boolean>] [-CatalogName <String>] [-CatalogUid <Int32>] [-ClientAddress <String>] [-ClientName <String>] [-ClientVersion <String>] [-ColorDepth <ColorDepth>] [-ConnectedViaHostName <String>] [-ConnectedViaIP <String>] [-ControllerDNSName <String>] [-DeliveryType <DeliveryType>] [-Description <String>] [-DesktopCondition <String>] [-DesktopGroupName <String>] [-DesktopGroupUid <Int32>] [-DesktopKind <DesktopKind>] [-DeviceId <String>] [-DNSName <String>] [-FunctionalLevel <FunctionalLevel>] [-HardwareId <String>] [-HostedMachineId <String>] [-HostedMachineName <String>] [-HostingServerName <String>] [-HypervisorConnectionName <String>] [-HypervisorConnectionUid <Int32>] [-IconUid <Int32>] [-ImageOutOfDate <Boolean>] [-InMaintenanceMode <Boolean>] [-IPAddress <String>] [-IsAssigned <Boolean>] [-IsPhysical <Boolean>] [-LastConnectionFailure <ConnectionFailureReason>] [-LastConnectionTime <DateTime>] [-LastConnectionUser <String>] [-LastDeregistrationReason <DeregistrationReason>] [-LastDeregistrationTime <DateTime>] [-LastErrorReason <String>] [-LastErrorTime <DateTime>] [-LastHostingUpdateTime <DateTime>] [-LaunchedViaHostName <String>] [-LaunchedViaIP <String>] [-MachineInternalState <MachineInternalState>] [-MachineUid <Int32>] [-OSType <String>] [-OSVersion <String>] [-PersistUserChanges <PersistUserChanges>] [-PowerActionPending <Boolean>] [-PowerState <PowerState>] [-Protocol <String>] [-ProvisioningType <ProvisioningType>] [-PublishedApplication <String>] [-PublishedName <String>] [-PvdStage <PvdStage>] [-RegistrationState <RegistrationState>] [-SecureIcaActive <Boolean>] [-SecureIcaRequired <Boolean>] [-SessionHidden <Boolean>] [-SessionId <Int32>] [-SessionState <SessionState>] [-SessionStateChangeTime <DateTime>] [-SessionUid <Int64>] [-SessionUserName <String>] [-SessionUserSID <String>] [-SID <String>] [-SmartAccessTag <String>] [-StartTime <DateTime>] [-SummaryState <DesktopSummaryState>] [-Tag <String>] [-WillShutdownAfterUse <Boolean>] [-ApplicationUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

This cmdlet is now deprecated, please use Get-BrokerMachine.

Retrieves desktops matching the specified criteria. If no parameters are specified this cmdlet enumerates all desktops.

Get-BrokerDesktop returns objects that combine desktop configuration and state information.

For single-session desktops, session information is displayed if present. It is possible that there are more than one sessions present on single-session desktops if 'fast user switching' is enabled, this cmdlet will prefer to return information about brokered sessions (rather than, for example, unbrokered direct RDP sessions). If there is no session running, session related fields return $null.

For multi-session desktops, no session information is ever displayed by this cmdlet, so session related fields always return $null. Get-BrokerSession can be used to get information about sessions on both multi-session and single-session desktops.

To count desktops, rather than retrieve full details of each desktop, use Group-BrokerDesktop instead.

For information about advanced filtering options, see about_Broker_Filtering; for information about desktops, see about_Broker_Desktops.

---------- BrokerDesktop Object

The desktop object returned represents a physical or virtual machine configured in the site that is able to run either a Microsoft Windows desktop environment, individual applications, or both.

-- AgentVersion (System.String)

Version of the Citrix Virtual Delivery Agent (VDA) installed on the desktop.

-- ApplicationsInUse (System.String[])

List of applications in use on the desktop (in the form of browser name).

-- AssignedClientName (System.String)

The name of the endpoint client device that the desktop has been assigned to.

-- AssignedIPAddress (System.String)

The IP address of the endpoint client device that the desktop has been assigned to.

-- AssociatedUserFullNames (System.String[])

Full names of the users that have been associated with the desktop (in the form "Firstname Lastname").

Associated users are the current user(s) for shared desktops and the assigned users for private desktops.

-- AssociatedUserNames (System.String[])

Usernames of the users that have been associated with the desktop (usually in the form "domain\user").

Associated users are the current user(s) for shared desktops and the assigned users for private desktops.

-- AssociatedUserUPNs (System.String[])

The user principal names of the users that have been associated with the desktop (in the form user@upndomain.com).

Associated users are the current user(s) for shared desktops and the assigned users for private desktops.

-- AutonomouslyBrokered (System.Boolean?)

Session property indicating if the current session is an HDX session established by direct connection without being brokered.

Session properties are always null for multi-session desktops.

-- CatalogName (System.String)

Name of the catalog the desktop is a member of.

-- CatalogUid (System.Int32)

UID of the catalog the desktop is a member of.

-- ClientAddress (System.String)

Session property indicating the IP address of the client connected to the desktop.

Session properties are always null for multi-session desktops.

-- ClientName (System.String)

Session property indicating the host name of the client connected to the desktop.

Session properties are always null for multi-session desktops.

-- ClientVersion (System.String)

Session property indicating the version of the Citrix Receiver running on the connected client.

Session properties are always null for multi-session desktops.

-- ColorDepth (Citrix.Broker.Admin.SDK.ColorDepth?)

The color depth setting configured on the desktop, possible values are:

$null, FourBit, EightBit, SixteenBit, and TwentyFourBit.

-- ConnectedViaHostName (System.String)

Session property indicating the host name of the connection gateway, router or client.

Session properties are always null for multi-session desktops.

-- ConnectedViaIP (System.String)

Session property indicating the IP address of the connection gateway, router or client.

Session properties are always null for multi-session desktops.

-- ControllerDNSName (System.String)

The DNS host name of the controller that the desktop is registered to.

-- DeliveryType (Citrix.Broker.Admin.SDK.DeliveryType)

Denotes whether the desktop delivers desktops only, apps only or both.

-- Description (System.String)

Description of the desktop.

-- DesktopConditions (System.String[])

List of outstanding desktop conditions for the desktop.

-- DesktopGroupName (System.String)

Name of the desktop group the desktop has been assigned to.

-- DesktopGroupUid (System.Int32)

Uid of the desktop group the desktop has been assigned to.

-- DesktopKind (Citrix.Broker.Admin.SDK.DesktopKind)

Deprecated.

Denotes whether the desktop is private or shared. AllocationType should be used instead.

-- DeviceId (System.String)

Session property indicating a unique identifier for the client device that has most recently been associated with the current session.

Session properties are always null for multi-session desktops.

-- DNSName (System.String)

The DNS host name of the desktop.

-- FunctionalLevel (Citrix.Broker.Admin.SDK.FunctionalLevel?)

The functional level of the desktop, if known.

-- HardwareId (System.String)

Session property indicating a unique identifier for the client hardware that has been most recently associated with the current session.

Session properties are always null for multi-sesison desktops.

-- HostedMachineId (System.String)

Unique ID within the hosting unit of the target managed desktop.

-- HostedMachineName (System.String)

The friendly name of a hosted desktop as used by its hypervisor. This is not necessarily the DNS name of the desktop.

-- HostingServerName (System.String)

DNS name of the hypervisor that is hosting the desktop if managed.

-- HypervisorConnectionName (System.String)

The name of the hypervisor connection that the desktop's hosting server is accessed through, if managed.

-- HypervisorConnectionUid (System.Int32?)

The UID of the hypervisor connection that the desktop's hosting server is accessed through, if managed.

-- IconUid (System.Int32?)

The UID of the desktop's icon that is displayed in StoreFront.

-- ImageOutOfDate (System.Boolean?)

Denotes whether the VM image for a hosted desktop is out of date.

-- InMaintenanceMode (System.Boolean)

Denotes whether the desktop is in maintenance mode.

-- IPAddress (System.String)

The IP address of the desktop.

-- IsAssigned (System.Boolean)

Denotes whether a private desktop has been assigned to a user/users, or a client name/address. Users can be assigned explicitly or by assigning on first use of the desktop.

-- IsPhysical (System.Boolean)

This value is true if the desktop is physical(ie not power managed by the Citrix Broker Service), and false otherwise.

-- LastConnectionFailure (Citrix.Broker.Admin.SDK.ConnectionFailureReason)

The reason for the last failed connection between a client and the desktop.

-- LastConnectionTime (System.DateTime?)

Time of the last detected connection attempt that either failed or succeeded.

-- LastConnectionUser (System.String)

The SAM name (in the form DOMAIN\user) of the user that last attempted a connection with the desktop. If the SAM name is not available, the SID is used.

-- LastDeregistrationReason (Citrix.Broker.Admin.SDK.DeregistrationReason?)

The reason for the last deregistration of the desktop with the broker. Possible values are:

AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

-- LastDeregistrationTime (System.DateTime?)

Time of the last deregistration of the desktop from the controller.

-- LastErrorReason (System.String)

The reason for the last error detected in the desktop.

-- LastErrorTime (System.DateTime?)

The time of the last detected error.

-- LastHostingUpdateTime (System.DateTime?)

Time of last update to any hosting data (such as power state) for this desktop reported by the hypervisor connection.

-- LaunchedViaHostName (System.String)

Session property that denotes the host name of the StoreFront server used to launch the current brokered session.

Session properties are always null for multi-session desktops.

-- LaunchedViaIP (System.String)

Session property that denotes the IP address of the StoreFront server used to launch the current brokered session.

Session properties are always null for multi-session desktops.

-- MachineInternalState (Citrix.Broker.Admin.SDK.MachineInternalState)

The internal state of the machine associated with the desktop; reported while the desktop is registered to a controller, plus some private Citrix Broker Service states while the machine is not registered.

-- MachineName (System.String)

DNS host name of the machine associated with the desktop.

-- MachineUid (System.Int32)

Uid of the associated machine.

-- OSType (System.String)

A string that can be used to identify the operating system that is running on the desktop.

-- OSVersion (System.String)

A string that can be used to identify the version of the operating system running on the desktop, if known

-- PersistUserChanges (Citrix.Broker.Admin.SDK.PersistUserChanges)

Describes whether/how the user changes are persisted. Possible values are:

o OnLocal - Persist the user changes on the local disk of the desktop.

o Discard - Discard user changes.

o OnPvd - Persist user changes on the Citrix Personal vDisk.

-- PowerActionPending (System.Boolean)

Property indicating whether there are any pending power actions for the desktop.

-- PowerState (Citrix.Broker.Admin.SDK.PowerState)

The current power state of the desktop. Possible values are: Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, resuming.

-- Protocol (System.String)

Session property that denotes the protocol that the current session is using, can be either HDX, RDP or Console. Console sessions on XenDesktop 5 VDAs appear with a blank protocol.

Session properties are always null for multi-session desktops.

-- ProvisioningType (Citrix.Broker.Admin.SDK.ProvisioningType)

Describes how the machine associated with the desktop was provisioned, possible values are:

o Manual: No automated provisioning.

o PVS: Machine provisioned by PVS (may be physical, blade, VM,...)

o MCS: Machine provisioned by MCS (machine must be VM)

-- PublishedApplications (System.String[])

List of applications published by the desktop (displayed as browser names).

-- PublishedName (System.String)

The name of the desktop that is displayed in StoreFront, if the desktop is published.

-- PvdStage (Citrix.Broker.Admin.SDK.PvdStage)

For a desktop supporting Personal vDisk technology (PvD), indicates the stage of the PvD image preparation.

-- RegistrationState (Citrix.Broker.Admin.SDK.RegistrationState)

Indicates the registration state of the desktop. Possible values are: Unregistered, Initializing, Registered, AgentError.

-- SecureIcaActive (System.Boolean?)

Session property that indicates whether SecureICA is active on the current session.

Session properties are always null for multi-session desktops.

-- SecureIcaRequired (System.Boolean?)

Flag indicating whether SecureICA is required or not when starting a session on the desktop.

-- SessionHidden (System.Boolean?)

Session property that indicates if a session is hidden.

Session properties are always null for multi-session desktops.

-- SessionId (System.Int32?)

Deprecated. A unique identifier that Remote Desktop Services uses to track the session but it is only unique on that machine and only unique at any one particular time.

-- SessionState (Citrix.Broker.Admin.SDK.SessionState?)

Session property indicating the state of the current session.

Session properties are always null for multi-session desktops, possible values are: Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession and Unknown.

-- SessionStateChangeTime (System.DateTime?)

Session property indicating the time of the last state change of the current session.

Session properties are always null for multi-session desktops.

-- SessionUid (System.Int64?)

Session property indicating the UID of the current session.

Session properties are always null for multi-session desktops.

-- SessionUserName (System.String)

Session property indicates the name of the current sessions' user (in the form DOMAIN\user).

Session properties are always null for multi-session desktops.

-- SessionUserSID (System.String)

Session property indicates the SID of the current sessions' user.

Session properties are always null for multi-session desktops.

-- SID (System.String)

The SID of the desktop.

-- SmartAccessTags (System.String[])

Session property that indicates the Smart Access tags for the current session.

Session properties are always null on multi-session desktops.

-- StartTime (System.DateTime?)

Session property that indicates the start time of the current session.

Session properties are always null on multi-session desktops.

-- SummaryState (Citrix.Broker.Admin.SDK.DesktopSummaryState)

Indicates the overall state of the desktop. The overall state is a result of other more specific states such as session state, registration state and power state. Possible values: Off, Unregistered, Available, Disconnected, InUse, Preparing.

-- Tags (System.String[])

A list of tags for the desktop.

-- Uid (System.Int32)

UID of the desktop object.

-- WillShutdownAfterUse (System.Boolean)

Flag indicating whether this desktop is tainted and will be shut down after all sessions on the desktop have ended. This flag should only ever be true on power managed, single-session

desktops.

Note: The desktop will not shut down if it is in maintenance mode, but will shut down after the desktop is taken out of maintenance mode.

Related topics

Group-BrokerMachine

Get-BrokerMachine

Parameters

-Uid<Int32>

Gets desktops with a specific UID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets desktops with a specific machine name (in the form 'domain\machine').

Required?	false
Default Value	
Accept Pipeline Input?	false

-AgentVersion<String>

Gets desktops with a specific Citrix Virtual Delivery Agent version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationInUse<String>

Gets desktops running a specified published application (identified by browser name).

String comparisons are case-insensitive.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedClientName<String>

Gets desktops assigned to a specific client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedIPAddress<String>

Gets desktops assigned to a specific client IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserFullName<String>

Gets desktops with an associated user identified by their full name (usually in the form 'first-name last-name').

Associated users are the current user for shared desktops, and the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserName<String>

Gets desktops with an associated user identified by their user name (in the form 'domain\user').

Associated users are the current user for shared desktops, and the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserUPN<String>

Gets desktops with an associated user identified by their User Principle Name (in the form 'user@domain').

Associated users are the current user for shared desktops, and the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AutonomouslyBrokered<Boolean>

Gets desktops according to whether their current session is autonomously brokered or not. Autonomously brokered sessions are HDX sessions established by direct connection without being brokered.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogName<String>

Gets desktops from the catalog with the specific name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogUid<Int32>

Gets desktops from a catalog with a specific UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientAddress<String>

Gets desktops with a specific client IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientName<String>

Gets desktops with a specific client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientVersion<String>

Gets desktops with a specific client version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Gets desktops configured with a specific color depth.

Valid values are FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectedViaHostName<String>

Gets desktops with a specific host name of the incoming connection. This is usually a proxy or Citrix Access Gateway server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectedViaIP<String>

Gets desktops with a specific IP address of the incoming connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ControllerDNSName<String>

Gets desktops with a specific DNS name of the controller they are registered with.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeliveryType<DeliveryType>

Gets desktops of a particular delivery type.

Valid values are AppsOnly, DesktopsOnly, DesktopsAndApps

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets desktops with a specific description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopCondition<String>

Gets desktop with an outstanding desktop condition condition.

Valid values are:

o CPU: Indicates the machine has high CPU usage

o ICALatency: Indicates the network latency is high

o UPMLogonTime: Indicates that the profile load time was high

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets desktops from a desktop group with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets desktops from a desktop group with the specified UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopKind<DesktopKind>

Deprecated: Use AllocationType parameter.

Gets desktops of a particular kind.

Valid values are Private, Shared.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeviceId<String>

Gets desktops with a specific client device ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets desktops with a specific DNS name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-FunctionalLevel<FunctionalLevel>

Gets desktops with a specific FunctionalLevel.

Valid values are L5, L7, L7_6

Required?	false
Default Value	
Accept Pipeline Input?	false

-HardwareId<String>

Gets desktops with a specific client hardware ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineId<String>

Gets desktops with a specific machine ID known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets desktops with a specific machine name known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostingServerName<String>

Gets desktops with a specific name of the hosting hypervisor server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionName<String>

Gets desktops with a specific name of the hosting hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets desktops with a specific UID of the hosting hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Gets desktops with a specific configured icon. Note that desktops with a null IconUid use the icon of the desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ImageOutOfDate<Boolean>

Gets desktops by whether their disk image is out of date (for machines provisioned using MCS only).

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Gets desktops with a specific InMaintenanceMode setting.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IPAddress<String>

Gets desktops with a specific IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsAssigned<Boolean>

Gets desktops according to whether they are assigned or not. Desktops may be assigned to one or more users or groups, a client IP address or a client endpoint name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsPhysical<Boolean>

Specifies if machines in the catalog can be power managed by the Citrix Broker Service. Where the power state of the machine cannot be controlled, specify $true, otherwise $false. Can only be specified together with a provisioning type of Pvs or Manual, or if used with the deprecated CatalogKind parameter only with Pvs or PvsPvd catalog kinds.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastConnectionFailure<ConnectionFailureReason>

Gets desktops with a specific reason for the last recorded connection failure. This value is None if the last connection was successful or if there has been no attempt to connect to the desktop yet.

Valid values are None, SessionPreparation, RegistrationTimeout, ConnectionTimeout, Licensing, Ticketing, and Other.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastConnectionTime<DateTime>

Gets desktops that last connected at a specific time. This is the time that the broker detected that the connection attempt either succeeded or failed.

Required?	false

Default Value	
Accept Pipeline Input?	false

-LastConnectionUser<String>

Gets desktops where a specific user name last attempted a connection (in the form 'domain\user').

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationReason<DeregistrationReason>

Gets desktops whose broker last recorded a specific deregistration reason.

Valid values are $null, AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationTime<DateTime>

Gets desktops by the time that they were last deregistered.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastErrorReason<String>

Gets desktops with the specified last error reason.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastErrorTime<DateTime>

Gets desktops with the specified last error time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastHostingUpdateTime<DateTime>

Gets desktops with a specific time that the hosting information was last updated.

Required?	false

Default Value	
Accept Pipeline Input?	false

-LaunchedViaHostName<String>

Gets desktops with a specific host name of the StoreFront server from which the user launched the session.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LaunchedViaIP<String>

Gets desktops with a specific IP address of the StoreFront server from which the user launched the session.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineInternalState<MachineInternalState>

Gets desktops with the specified internal machine state.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineUid<Int32>

Gets desktops with a specific machine UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets desktops by the type of operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSVersion<String>

Gets desktops by the version of the operating system they are running.

Required?	false

Default Value	
Accept Pipeline Input?	false

-PersistUserChanges<PersistUserChanges>

Gets desktops by the location where the user changes are persisted.

o OnLocal - User changes are persisted locally.

o Discard - User changes are discarded.

o OnPvd - User changes are persisted on the Pvd.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerActionPending<Boolean>

Gets desktops with a specific power action pending state.

Valid values are $true or $false.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerState<PowerState>

Gets desktops with a specific power state.

Valid values are Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Protocol<String>

Gets desktops with connections using a specific protocol, for example HDX, RDP, or Console.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningType<ProvisioningType>

Gets desktops that are in a catalog with a particular provisioning type. Values can be:

o Manual - No provisioning.

o PVS - Machine provisioned by PVS (machine may be physical, blade, VM,...).

o MCS - Machine provisioned by MCS (machine must be VM).

Required?	false
Default Value	

Accept Pipeline Input?	false

-PublishedApplication<String>

Gets desktops with a specific application published to them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Gets desktops with a specific published name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdStage<PvdStage>

Gets desktops with a specific personal vDisk stage.

Valid values are None, Requested, Starting, Working and Failed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RegistrationState<RegistrationState>

Gets desktops with a specific registration state.

Valid values are Unregistered, Initializing, Registered and AgentError.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaActive<Boolean>

Gets desktops depending on whether the current session uses SecureICA or not.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Gets desktops configured with a particular SecureIcaRequired setting. Note that the desktop setting of $null indicates that the desktop group value is used.

Session properties are always null for multi-session desktops.

Required?	false

Default Value	
Accept Pipeline Input?	false

-SessionHidden<Boolean>

Gets desktops by whether their sessions are hidden or not. Hidden sessions are treated as though they do not exist when launching sessions; a hidden session cannot be reconnected to, but a new session may be launched using the same entitlement.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionId<Int32>

Deprecated.

Gets desktops by session ID, a unique identifier that Remote Desktop Services uses to track the session but it is only unique on that machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionState<SessionState>

Gets desktops with a specific session state.

Valid values are $null, Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession, and Unknown.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionStateChangeTime<DateTime>

Gets desktops whose sessions last changed state at a specific time.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUid<Int64>

Gets single-session desktops with a specific session UID ($null for no session).

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUserName<String>

Gets desktops with a specific user name for the current session (in the form 'domain\user').

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUserSID<String>

Gets desktops with a specific SID of the current session user.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SID<String>

Gets desktops with a specific machine SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SmartAccessTag<String>

Gets session desktops where the session has the specific SmartAccess tag.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartTime<DateTime>

Gets desktops with a specific session start time.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SummaryState<DesktopSummaryState>

Gets desktops with a specific summary state.

Valid values are Off, Unregistered, Available, Disconnected, InUse and Preparing.

Required?	false
Default Value	

Accept Pipeline Input?	false

-Tag<String>

Gets desktops with a specific tag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WillShutdownAfterUse<Boolean>

Gets desktops depending on whether they shut down after use or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationUid<Int32>

Gets desktops with a specific published application (identified by its UID).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Desktop

Get-BrokerDesktop returns an object for each matching desktop.

Notes

To compare dates or times, use -Filter and relative comparisons. For more information, see about_Broker_Filtering and the examples.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerDesktop -RegistrationState Unregistered
C:\PS> Get-BrokerDesktop -Filter { RegistrationState -ne 'Registered' }
```
Both commands retrieve desktops that are unregistered. The second command also includes desktops with a registration state of AgentError.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerDesktop -SessionUid $null | ft -a DNSName,SummaryState
```
Gets desktops without sessions, listing the DNS name and current state.

---------- EXAMPLE 3 ----------

```
C:\PS> Get-BrokerDesktop -Filter { OSType -like "Windows XP*" -and ImageOutOfDate }
```
Finds all Windows XP desktops with an out-of-date image.

-------------------------- EXAMPLE 4 --------------------------

C:\PS> Get-BrokerDesktop -ApplicationInUse '*powerpoint*'
Gets desktops running a published PowerPoint application. It matches any application browser name containing the word 'powerpoint'. String comparisons are case-insensitive.

-------------------------- EXAMPLE 5 --------------------------

C:\PS> Get-BrokerDesktop -DesktopCondition * DNSName,SessionUserName,DesktopConditions
Finds all desktops with an outstanding desktop condition, listing the affected desktop and user.

-------------------------- EXAMPLE 6 --------------------------

C:\PS> $d = (Get-Date).AddDays(-1)
C:\PS> Get-BrokerDesktop -Filter { StartTime -le $d } | ft MachineName,SessionUserName,StartTime,@{Label='Duration'; Expression={(Get-Date) - $_.StartTime}}
Finds users who have been logged on for more than a day, and outputs the machine name, start time, and duration the session has been logged on.

Get-BrokerDesktopGroup

Sep 10, 2014

Gets broker desktop groups configured for this site.

Syntax

Get-BrokerDesktopGroup [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerDesktopGroup [[-Name] <String>] [-AutomaticPowerOnForAssigned <Boolean>] [-AutomaticPowerOnForAssignedDuringPeak <Boolean>] [-ColorDepth <ColorDepth>] [-DeliveryType <DeliveryType>] [-Description <String>] [-DesktopKind <DesktopKind>] [-Enabled <Boolean>] [-InMaintenanceMode <Boolean>] [-IsRemotePC <Boolean>] [-Metadata <String>] [-MinimumFunctionalLevel <FunctionalLevel>] [-OffPeakBufferSizePercent <Int32>] [-OffPeakDisconnectAction <SessionChangeHostingAction>] [-OffPeakDisconnectTimeout <Int32>] [-OffPeakExtendedDisconnectAction <SessionChangeHostingAction>] [-OffPeakExtendedDisconnectTimeout <Int32>] [-OffPeakLogOffAction <SessionChangeHostingAction>] [-OffPeakLogOffTimeout <Int32>] [-PeakBufferSizePercent <Int32>] [-PeakDisconnectAction <SessionChangeHostingAction>] [-PeakDisconnectTimeout <Int32>] [-PeakExtendedDisconnectAction <SessionChangeHostingAction>] [-PeakExtendedDisconnectTimeout <Int32>] [-PeakLogOffAction <SessionChangeHostingAction>] [-PeakLogOffTimeout <Int32>] [-PublishedName <String>] [-ScopeId <Guid>] [-ScopeName <String>] [-SecureIcaRequired <Boolean>] [-SessionSupport <SessionSupport>] [-SettlementPeriodBeforeAutoShutdown <TimeSpan>] [-ShutdownDesktopsAfterUse <Boolean>] [-Tag <String>] [-TimeZone <String>] [-TotalApplications <Int32>] [-TurnOnAddedMachine <Boolean>] [-UUID <Guid>] [-ApplicationUid <Int32>] [-TagUid <Int32>] [-PowerTimeSchemeUid <Int32>] [-MachineConfigurationUid <Int32>] [-RemotePCCatalogUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieve desktop groups matching the specified criteria. If no parameters are specified this cmdlet enumerates all desktop groups.

Desktop groups represent groups of desktops that are managed together for brokering purposes.

---------- BrokerDesktopGroup Object

A desktop group object represents a collection of machines that are fully configured in a site that is able to run either a Microsoft Windows desktop environment, individual applications, or both.

-- AutomaticPowerOnForAssigned (System.Boolean)

Specifies whether assigned desktops in the desktop group are automatically started at the start of peak time periods. Only relevant for groups whose DesktopKind is Private.

-- AutomaticPowerOnForAssignedDuringPeak (System.Boolean)

Specifies whether assigned desktops in the desktop are automatically started throughout peak time periods. Only relevant

for groups whose DesktopKind is Private and which have AutomaticPowerOnForAssigned set to true.

-- ColorDepth (Citrix.Broker.Admin.SDK.ColorDepth)

Default color depth of sessions started with machines in the desktop group. Possible values are:

FourBit, EightBit, SixteenBit, TwentyFourBit.

-- ConfigurationSlotUids (System.Int32[])

Uids of any configuration slots which hold machine configurations associated with the desktop group. The order of slot UIDs in this list correspond with the order of items in the associated MachineConfigurationNames and MachineConfigurationUids list properties, and so the same slot UID can appear more than once.

-- DeliveryType (Citrix.Broker.Admin.SDK.DeliveryType)

The type of resources being published. Possible values are:

DesktopsOnly, AppsOnly, DesktopsAndApps.

-- Description (System.String)

Description of the desktop group.

-- DesktopKind (Citrix.Broker.Admin.SDK.DesktopKind)

The kind of the desktops being published, possible values are:

Private and Shared.

-- DesktopsAvailable (System.Int32)

The number of machines in the desktop group in state Available; this is the number of machines with no sessions present.

-- DesktopsDisconnected (System.Int32)

The number of disconnected sessions present on machines in the desktop group.

-- DesktopsInUse (System.Int32)

The number of machines in the desktop group in state InUse; this is the number of machines with at least one session present.

-- DesktopsNeverRegistered (System.Int32)

The number of machines in the desktop group that have never registered with the current site.

-- DesktopsPreparing (System.Int32)

The number of machines in the desktop group whose PvD disk image is being prepared.

-- DesktopsUnregistered (System.Int32)

The number of machines in the desktop group that are currently unregistered.

-- Enabled (System.Boolean)

Specifies whether the desktop group is enabled or not; disabled desktop groups do not appear to users.

-- IconUid (System.Int32)

The Uid of the icon to be used as a default for desktops in the desktop group. Individual desktop objects can override this default by setting the IconUid parameter on the desktop object.

-- InMaintenanceMode (System.Boolean)

Specifies whether the machines in the desktop group are in maintenance mode or not.

-- IsRemotePC (System.Boolean)

Specifies whether the desktop group is a Remote PC desktop group.

-- MachineConfigurationNames (System.String[])

The MachineConfiguration names associated with the desktop group.

-- MachineConfigurationUids (System.Int32[])

The MachineConfiguration uids associated with the desktop group.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Metadata associated with the desktop group.

-- MinimumFunctionalLevel (Citrix.Broker.Admin.SDK.FunctionalLevel)

The minimum FunctionalLevel required for the machines in the desktop group to be able to register with the Citrix Broker Service.

-- Name (System.String)

Name of the desktop group.

-- OffPeakBufferSizePercent (System.Int32)

The percentage of machines that are kept available in an idle state outside peak hours.

-- OffPeakDisconnectAction (Citrix.Broker.Admin.SDK.SessionChangeHostingAction)

The action that is performed after a configurable period of a user session disconnecting outside peak hours. Possible values are Nothing, Suspend or Shutdown.

-- OffPeakDisconnectTimeout (System.Int32)

The number of minutes before the configured action is performed after a user session disconnects outside peak hours.

-- OffPeakExtendedDisconnectAction (Citrix.Broker.Admin.SDK.SessionChangeHostingAction)

The action performed after a second configurable period of a user session disconnecting outside peak hours. Possible values are Nothing, Suspend, or Shutdown.

-- OffPeakExtendedDisconnectTimeout (System.Int32)

The number of minutes before the second configured action is performed after a user session disconnects outside peak hours.

-- OffPeakLogOffAction (Citrix.Broker.Admin.SDK.SessionChangeHostingAction)

The action performed after a configurable period of a user session ending outside peak hours. Possible values are Nothing, Suspend, or Shutdown.

-- OffPeakLogOffTimeout (System.Int32)

The number of minutes before the configured action is performed after a user session ends outside peak hours.

-- PeakBufferSizePercent (System.Int32)

The percentage of machines in the desktop group that are kept available in an idle state in peak hours.

-- PeakDisconnectAction (Citrix.Broker.Admin.SDK.SessionChangeHostingAction)

The action performed after a configurable period of a user session disconnecting in peak hours. Possible values are Nothing, Suspend, or Shutdown.

-- PeakDisconnectTimeout (System.Int32)

The number of minutes before the configured action is performed after a user session disconnects in peak hours.

-- PeakExtendedDisconnectAction (Citrix.Broker.Admin.SDK.SessionChangeHostingAction)

The action performed after a second configurable period of a user session disconnecting in peak hours. Possible values are Nothing, Suspend, or Shutdown.

-- PeakExtendedDisconnectTimeout (System.Int32)

The number of minutes before the second configured action is performed after a user session disconnects in peak hours.

-- PeakLogOffAction (Citrix.Broker.Admin.SDK.SessionChangeHostingAction)

The action performed after a configurable period of a user session ending in peak hours. Possible values are Nothing, Suspend, or Shutdown.

-- PeakLogOffTimeout (System.Int32)

The number of minutes before the configured action is performed after a user session ends in peak hours.

-- ProtocolPriority (System.String[])

A list of protocol names in the order in which they are attempted for use during connection.

-- PublishedName (System.String)

The name of the desktop group as it is to appear to the user in StoreFront.

-- Scopes (Citrix.Broker.Admin.SDK.ScopeReference[])

The list of the delegated admin scopes to which the desktop group belongs.

-- SecureIcaRequired (System.Boolean)

Flag that specifies if the SecureICA encryption of the HDX protocol is required for sessions of desktops in the desktop group.

-- Sessions (System.Int32)

The total number of user sessions currently running on all of the machines in the desktop group.

-- SessionSupport (Citrix.Broker.Admin.SDK.SessionSupport)

Specifies the session support (single/multi) of the machines in the desktop group. Machines with the incorrect session support for the desktop group will be unable to register with the Citrix Broker Service.

-- SettlementPeriodBeforeAutoShutdown (System.TimeSpan)

Time after a session ends during which automatic shutdown requests (for example, shutdown after use, idle pool management) are deferred. Any outstanding shutdown request takes effect after the settlement period expires. This is typically used to configure time to allow logoff scripts to complete.

-- ShutdownDesktopsAfterUse (System.Boolean)

Specifies if the desktops will shut down after they have been used and there are no sessions running on the machine. The machines will not shut down if they are placed into maintenance mode, even if this flag is set to $true. The machines, however, will shutdown after the machine is taken out of maintenance mode if the flag is still set.

-- Tags (System.String[])

Tags associated with the desktop group.

-- TimeZone (System.String)

The timezone that desktops in the desktop group are in (for power policy purposes).

-- TotalApplications (System.Int32)

Total number of applications associated with the desktop group.

-- TotalDesktops (System.Int32)

Total number of machines in the desktop group.

-- TurnOnAddedMachine (System.Boolean)

Specifies whether the broker should attempt to turn on power-managed machines when they are added to the desktop group.

-- Uid (System.Int32)

Uid of the desktop group.

-- UUID (System.Guid)

UUID if the desktop group.

Related topics

New-BrokerDesktopGroup

Set-BrokerDesktopGroup

Rename-BrokerDesktopGroup

Remove-BrokerDesktopGroup

Add-BrokerUser

Add-BrokerTag

Parameters

-Uid<Int32>

Gets desktop groups with the specified value of Uid.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets desktop groups whose name matches the supplied pattern.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AutomaticPowerOnForAssigned<Boolean>

Gets only desktop groups with the specified value of AutomaticPowerOnForAssigned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AutomaticPowerOnForAssignedDuringPeak<Boolean>

Gets only desktop groups with the specified value of AutomaticPowerOnForAssignedDuringPeak.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Gets only desktop groups with the specified color depth.

Valid values are FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeliveryType<DeliveryType>

Gets desktop groups according to their delivery type.

Valid values are DesktopsOnly, AppsOnly and DesktopsAndApps.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets desktop groups whose description matches the supplied pattern.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopKind<DesktopKind>

Gets desktops of a particular kind.

Valid values are Private and Shared.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets desktop groups with the specified value of Enabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Gets desktop groups with the specified value of InMaintenanceMode.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsRemotePC<Boolean>

Gets desktop groups with the specified IsRemotePC value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-MinimumFunctionalLevel<FunctionalLevel>

Gets desktop groups with a specific MinimumFunctionalLevel.

Valid values are L5, L7, L7_6

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakBufferSizePercent<Int32>

Gets desktop groups with the specified value of OffPeakBufferSizePercent.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakDisconnectAction<SessionChangeHostingAction>

Gets desktop groups with the specified value of OffPeakDisconnectAction.

Required?	false
Default Value	

Accept Pipeline Input?	false

-OffPeakDisconnectTimeout<Int32>

Gets desktop groups with the specified value of OffPeakDisconnectTimeout.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakExtendedDisconnectAction<SessionChangeHostingAction>

Gets desktop groups with the specified value of OffPeakExtendedDisconnectAction.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakExtendedDisconnectTimeout<Int32>

Gets desktop groups with the specified value of OffPeakExtendedDisconnectTimeout.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakLogOffAction<SessionChangeHostingAction>

Gets desktop groups with the specified value of OffPeakLogOffAction.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakLogOffTimeout<Int32>

Gets desktop groups with the specified value of OffPeakLogOffTimeout.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakBufferSizePercent<Int32>

Gets desktop groups with the specified value of PeakBufferSizePercent.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakDisconnectAction<SessionChangeHostingAction>

Gets desktop groups with the specified value of PeakDisconnectAction.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakDisconnectTimeout<Int32>

Gets desktop groups with the specified value of PeakDisconnectTimeout.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakExtendedDisconnectAction<SessionChangeHostingAction>

Gets desktop groups with the specified value of PeakExtendedDisconnectAction.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakExtendedDisconnectTimeout<Int32>

Gets desktop groups with the specified value of PeakExtendedDisconnectTimeout.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakLogOffAction<SessionChangeHostingAction>

Gets desktop groups with the specified value of PeakLogOffAction.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakLogOffTimeout<Int32>

Gets desktop groups with the specified value of PeakLogOffTimeout.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Gets desktop groups whose published name matches the supplied pattern.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScopeId<Guid>

Gets desktop groups that are associated with the given scope identifier.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScopeName<String>

Gets desktop groups that are associated with the given scope name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Gets desktop groups with the specified value of SecureIcaRequired.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSupport<SessionSupport>

Gets desktop groups that have the specified session capability. Values can be:

o SingleSession - Single-session only machine.

o MultiSession - Multi-session capable machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SettlementPeriodBeforeAutoShutdown<TimeSpan>

Gets desktop groups with the specified value of SettlementPeriodBeforeAutoShutdown.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ShutdownDesktopsAfterUse<Boolean>

Gets desktop groups with the specified value of ShutdownDesktopsAfterUse.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Tag<String>

Gets desktop groups tagged with the specified tag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TimeZone<String>

Gets desktop groups with the specified value of TimeZone.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TotalApplications<Int32>

Gets desktop groups that are acting as delivery groups for the specified number of applications.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TurnOnAddedMachine<Boolean>

Gets desktop groups with the specified value of TurnOnAddedMachine value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UUID<Guid>

Gets desktop groups with the specified value of UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationUid<Int32>

Gets desktop groups that publish the specified application (identified by Uid)

Required?	false
Default Value	
Accept Pipeline Input?	false

-TagUid<Int32>

Gets desktop groups to which the specified tag (identified by its Uid) has been added to help identify it - see Add-BrokerTag for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerTimeSchemeUid<Int32>

Gets desktop groups associated with the specified power time scheme (identified by its Uid).

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineConfigurationUid<Int32>

Gets desktop groups with the specified value of MachineConfiguration.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemotePCCatalogUid<Int32>

Gets Remote PC desktop groups associated with the specified catalog.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or

spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.DesktopGroup

Get-BrokerDesktopGroup returns an object for each matching desktop group.

Notes

To perform greater-than or less-than comparisons, use -Filter. For more information, see about_Broker_Filtering and the examples.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerDesktopGroup -PublishedName EMEA*
```

Finds all desktop groups with published names starting with "EMEA".

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerDesktopGroup -InMaintenanceMode $true
```

Finds all desktop groups in maintenance mode.

Get-BrokerDesktopUsage

Sep 10, 2014

Get usage history of desktop groups.

Syntax

Get-BrokerDesktopUsage [-DesktopGroupName <String>] [-DesktopGroupUid <Int32>] [-InUse <Int32>] [-Timestamp <DateTime>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns information, recorded by the broker on an hourly basis, about the number of desktops in use for each desktop group. Analyzing the historical usage records can give some guidance on usage patterns and help choosing idle pool settings.

Without parameters, Get-BrokerDesktopUsage returns the first 250 records. By using parameters, you can be more selective about the records that are returned.

To retrieve more than the default 250 records, use the -MaxRecordCount parameter. To select data for a specific desktop group, use either the -DesktopGroupName or -DesktopGroupUid parameters.

See the examples for this cmdlet and about_Broker_Filtering for details of how to perform advanced filtering.

---------- BrokerDesktopUsage Object

Desktop usage object contains information to tell how many desktops in a desktop group are in use at a given time (identified by a timestamp).

-- DesktopGroupUid (System.Int32)

Uid of the desktop group that the usage data corresponds to.

-- InUse (System.Int32)

Specifies how many desktop are in use at the time the timestamp corresponds to.

-- Timestamp (System.DateTime)

Date and time the desktop usage information corresponds to.

Related topics

Parameters

-DesktopGroupName<String>

Gets usage records for the named desktop group or for multiple desktop groups if wildcards have been specified.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets usage records for a specific desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InUse<Int32>

Gets usage records where the in-use count matches the specified value. This is useful when checking for zero or when used inside a -Filter expression.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Timestamp<DateTime>

Gets usage records that occurred at the given time.

In general, Citrix recommends, using -Filter and relative comparisons. For a demonstration, see the examples.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe objects to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.DesktopUsage

Get-BrokerDesktopUsage returns an object for each matching record.

Notes

Desktop usage information is automatically deleted after 7 days.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerDesktopUsage -DesktopGroupName TestGroup -MaxRecordCount 24 -SortBy '-Timestamp' | ft -a @{Name='Time';Expression={'{0:t}' -f $_.Timestamp}},I
```

Returns the last 24 hours of usage information for desktop group TestGroup, formatting it as two columns labeled Time and InUse.

---------- EXAMPLE 2 ----------

```
C:\PS> $d = Get-Date -Hour 0 -Minute 0 -Second 0
C:\PS> Get-BrokerDesktopUsage -Filter { DesktopGroupName -eq 'TestGroup' -and Timestamp -ge $d }
```

Returns today's usage information for desktop group TestGroup.

---------- EXAMPLE 3 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup TestGroup
C:\PS> Get-BrokerDesktopUsage -DesktopGroupUid $dg.Uid | Select Timestamp,InUse,@{Name='Percent';Expression={'{0:P0}' -f ($_.InUse / $dg.TotalDesktops)}}
```

Retrieves the usage history for desktop group TestGroup and adds a column showing the number of desktops in that group in use, as a percentage.

Get-BrokerEntitlementPolicyRule

Sep 10, 2014

Gets desktop rules from the site's entitlement policy.

Syntax

Get-BrokerEntitlementPolicyRule [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerEntitlementPolicyRule [[-Name] <String>] [-BrowserName <String>] [-ColorDepth <ColorDepth>] [-Description <String>] [-DesktopGroupUid <Int32>] [-Enabled <Boolean>] [-ExcludedUser <User>] [-ExcludedUserFilterEnabled <Boolean>] [-IconUid <Int32>] [-IncludedUser <User>] [-IncludedUserFilterEnabled <Boolean>] [-Metadata <String>] [-PublishedName <String>] [-SecureIcaRequired <Boolean>] [-SessionReconnection <SessionReconnection>] [-UUID <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns desktop rules matching the specified search criteria from the site's entitlement policy. If no search criteria are specified, all desktop rules in the entitlement policy are obtained.

A desktop rule in the entitlement policy defines the users who are allowed per-session access to a machine from the rule's associated desktop group to run a full desktop session.

---------- BrokerEntitlementPolicyRule Object

The BrokerEntitlementPolicyRule object represents a single desktop rule within the site's entitlement policy. It contains the following properties:

-- BrowserName (System.String)

Site-wide unique name identifying this desktop entitlement to other components (for example StoreFront).

-- ColorDepth (Citrix.Broker.Admin.SDK.ColorDepth?)

The color depth of any desktop session launched by the user from the entitlement. If null, the equivalent setting from the rule's desktop group is used.

-- Description (System.String)

Optional description of the rule. The text may be visible to the end user, for example, as a tooltip associated with the desktop entitlement.

-- DesktopGroupUid (System.Int32)

The unique ID of the desktop group to which the rule applies.

-- Enabled (System.Boolean)

Indicates whether the rule is enabled. A disabled rule is ignored when evaluating the site's entitlement policy.

-- ExcludedUserFilterEnabled (System.Boolean)

Indicates whether the excluded users filter is enabled. If the filter is disabled then any user entries in the filter are ignored when entitlement policy rules are evaluated.

-- ExcludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

The excluded users filter of the rule, that is, the users and groups who are explicitly denied an entitlement to a desktop session from this rule.

-- IconUid (System.Int32?)

The unique ID of the icon used to display the desktop entitlement to the user. If null, the equivalent setting from the rule's desktop group is used.

-- IncludedUserFilterEnabled (System.Boolean)

Indicates whether the included users filter is enabled. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to a desktop session by the rule.

-- IncludedUsers (Citrix.Broker.Admin.SDK.ChbUser[])

The included users filter of the rule, that is, the users and groups who are granted an entitlement to a desktop session by the rule.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

A collection of arbitrary key/value pairs that can be associated with the rule. The administrator can use these values for any purpose; they are not used by the site itself in any way.

-- Name (System.String)

The administrative name of the rule. Each rule in the site's entitlement policy must have a unique name (irrespective of whether they are desktop or application rules).

-- PublishedName (System.String)

The name of the desktop session entitlement as seen by the user. If null, the equivalent setting from the rule's desktop group is used.

-- SecureIcaRequired (System.Boolean?)

Indicates whether the rule requires the SecureICA protocol for desktop sessions launched using the entitlement. If null, the equivalent setting from the rule's desktop group is used.

-- SessionReconnection (Citrix.Broker.Admin.SDK.SessionReconnection)

Defines reconnection (roaming) behavior for sessions launched using this rule. Session reconnection control is an experimental and unsupported feature.

-- Uid (System.Int32)

The unique ID of the rule itself.

-- UUID (System.Guid)

UUID of the rule.

Related topics

New-BrokerEntitlementPolicyRule

Set-BrokerEntitlementPolicyRule

Rename-BrokerEntitlementPolicyRule

Remove-BrokerEntitlementPolicyRule

Parameters

-Uid<Int32>

Gets the desktop rule with the specified unique ID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets only desktop rules with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrowserName<String>

Gets only desktop rules with browser names matching the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Gets only desktop rules with the specified color depth.

Valid values are $null, FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets only desktop rules with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets only desktop rules that apply to the desktop group with the specified unique ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets only desktop rules that are in the specified state, either enabled ($true), or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUser<User>

Gets only desktop rules that have the specified user in their excluded users filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Gets only desktop rules that have their excluded user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Gets only desktop rules using the icon with the specified unique ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUser<User>

Gets only desktop rules that have the specified user in their included users filter (whether the filter is enabled or not).

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Gets only desktop rules that have their included user filter enabled ($true) or disabled ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Gets only desktop rules with the specified published name, that is, the desktop session entitlement name that the end user sees.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Gets only desktop rules that require the desktop session to use the SecureICA protocol ($true) or not ($false).

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionReconnection<SessionReconnection>

Gets only desktop rules with the specified session reconnection behavior.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UUID<Guid>

Gets rules with the specified value of UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.EntitlementPolicyRule

Get-BrokerEntitlementPolicyRule returns all desktop entitlement policy rules that match the specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerEntitlementPolicyRule
```

Returns all desktop rules from the entitlement policy. This offers a complete description of the current site's entitlement policy with respect to desktops published from shared desktop groups.

---------- EXAMPLE 2 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Customer Support'
C:\PS> Get-BrokerEntitlementPolicyRule -DesktopGroupUid $dg.Uid
```

Returns all desktop rules in the entitlement policy that give users entitlements to desktop sessions in the Customer Support desktop group.

Get-BrokerHostingPowerAction

Sep 10, 2014

Gets power actions queued for machines.

Syntax

```
Get-BrokerHostingPowerAction [-Uid] <Int64> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerHostingPowerAction [[-MachineName] <String>] [-Action <PowerManagementAction>] [-ActionCompletionTime <DateTime>] [-ActionStartTime <DateTime>] [-ActualPriority <Int32>] [-BasePriority <Int32>] [-DNSName <String>] [-FailureReason <String>] [-HostedMachineName <String>] [-HypervisorConnectionName <String>] [-HypervisorConnectionUid <Int32>] [-Metadata <String>] [-RequestTime <DateTime>] [-State <PowerActionState>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Finds power actions matching the specified search criteria from the queue of all known power actions. These power actions can be waiting to be dealt with or can be part way through being processed by the relevant hypervisor, or they can be recently completed actions. Completed actions are removed from the queue after a configured period, the default being one hour.

If no search criteria are specified all actions in the queue are obtained.

A Hosting Power Action record defines the action that is to be performed or has been performed, the machine that the action is to be applied to, the priority of the action in relation to other actions in the queue, times for points in the life of the action, and any results if the action has completed.

For a detailed description of the queuing mechanism, see 'help about_Broker_PowerManagement'.

---------- BrokerHostingPowerAction Object

The BrokerHostingPowerAction object represents an instance of a power action. It contains the following properties:

-- Action (Citrix.Broker.Admin.SDK.PowerManagementAction)

The power action to be performed. Possible values are: TurnOn, TurnOff, Shutdown, Reset, Restart, Suspend, Resume.

-- ActionCompletionTime (System.DateTime?)

The time when the power action was completed by the hypervisor connection.

-- ActionStartTime (System.DateTime?)

The time when the power action was started to be processed by the hypervisor.

-- ActualPriority (System.Int32)

The current priority of the operation after any priority boosting.

-- BasePriority (System.Int32)

The starting priority of the operation.

-- DNSName (System.String)

The fully qualified DNS name of the machine that the power action applies to.

-- FailureReason (System.String)

For failed power actions, an indication of the reason for the failure.

-- HostedMachineName (System.String)

The hypervisor's name for the machine that the power action applies to.

-- HypervisorConnectionUid (System.Int32)

The unique identifier of the hypervisor connection that is associated with the target machine.

-- MachineName (System.String)

The name of the machine that the power action applies to, in the form domain\machine.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Metadata for this power action.

-- RequestTime (System.DateTime)

The timestamp of when the action was created and placed in the queue.

-- State (Citrix.Broker.Admin.SDK.PowerActionState)

The current state of this power action. Possible values are: Pending, Started, Completed, Failed, Canceled, Deleted, Lost.

-- Uid (System.Int64)

The unique identifier of the power action.

Related topics

New-BrokerHostingPowerAction

Set-BrokerHostingPowerAction

Remove-BrokerHostingPowerAction

Parameters

-Uid<Int64>

Gets only the single action record whose ID matches the specified value.

Required?	true

Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets only the records for actions that are for machines whose name (of the form domain\machine) matches the specified string.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Action<PowerManagementAction>

Gets only action records with the specified action type.

Valid values are TurnOn, TurnOff, ShutDown, Reset, Restart, Suspend and Resume.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ActionCompletionTime<DateTime>

Gets only action records reported as having completed successfully at the specified time. This is useful with advanced filtering; for more information, see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ActionStartTime<DateTime>

Gets only action records reported as starting to be processed by the relevant hypervisor at the specified time. This is useful with advanced filtering; for more information, see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ActualPriority<Int32>

Gets only the records for actions whose current active priority matches the specified value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BasePriority<Int32>

Gets only the records for actions whose original priority matches the specified value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets only the records for actions that are for machines whose DNS name matches the specified string.

Required?	false
Default Value	
Accept Pipeline Input?	false

-FailureReason<String>

Gets only the records for actions that have failed and whose failure reason string matches the specified string.

Required?	false

Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets only the records for actions that are for machines whose Hosting Name (the machine name as understood by by the hypervisor) matches the specified string.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionName<String>

Gets only the records for actions for machines hosted via a hypervisor connection whose name matches the specified string.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets only the records for actions for machines hosted via a hypervisor connection whose ID matches the specified value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata

"abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-RequestTime<DateTime>

Gets only the records for actions created and added to the queue at the specified time. This is useful with advanced filtering; for more information, see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-State<PowerActionState>

Gets only the records for actions with the specified current state.

Valid values are Pending, Started, Completed, Failed, Canceled, Deleted and Lost.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	

Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.HostingPowerAction

Get-BrokerHostingPowerAction returns all power actions that match the specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerHostingPowerAction
Fetches records for all known power actions either waiting to be processed, or currently being processed, or which have been processed in the last hour.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerHostingPowerAction -State Pending -HypervisorConnectionName 'XenPool5'
Fetches records for all power actions that are waiting to be processed and where the action is for a virtual machine that is hosted by the hypervisor called 'XenPool5'.

Get-BrokerHypervisorAlert

Sep 10, 2014

Gets hypervisor alerts recorded by the controller.

Syntax

```
Get-BrokerHypervisorAlert -Uid <Int64> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerHypervisorAlert [-HostingServerName <String>] [-HypervisorConnectionUid <Int32>] [-Metadata <String>] [-Metric <AlertMetric>] [-Severity <AlertSeverity>] [-Time <DateTime>] [-TriggerInterval <TimeSpan>] [-TriggerLevel <Double>] [-TriggerPeriod <TimeSpan>] [-TriggerValue <Double>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Get-BrokerHypervisorAlert cmdlet gets alert objects reported by the hypervisors that the controller is monitoring.

Without parameters, Get-BrokerHypervisorAlert gets all of the alerts recorded. Use parameters to select which alerts are returned.

Once you have configured suitable alerts in your hypervisor, and configured the controller with your hypervisor details (see New-BrokerHypervisorConnection), the controller monitors each hypervisor for new alerts.

Four hypervisor alert metrics are recorded; these relate to the hypervisor host, not individual virtual machines:

-- Cpu: Reports excessive CPU usage.

-- Memory: Reports excessive memory usage.

-- Network: Reports high network activity.

-- Disk: Reports high disk activity.

Each alert also includes information about where and when the alert occurred, the severity of the alert (Red/Yellow), and the configuration of the triggered alert.

The following metrics are supported with these hypervisors:

-- VMware ESX (Cpu, Memory, Network, Disk)

-- Citrix XenServer (Cpu, Network)

-- Microsoft Hyper-V (None)

---------- BrokerHypervisorAlert Object

The BrokerHypervisorAlert represents a hypervisor alert object. It contains the following properties:

-- HostingServerName (System.String)

The name of the hypervisor hosting this machine.

-- HypervisorConnectionUid (System.Int32)

The Uid of the hypervisor connection that reported this alert.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Metadata for this hypervisor alert.

-- Metric (Citrix.Broker.Admin.SDK.AlertMetric)

The metric this alert relates to: Cpu, Memory, Network or Disk.

-- Severity (Citrix.Broker.Admin.SDK.AlertSeverity)

Severity of the alert (Red or Yellow). Red is more serious than Yellow.

-- Time (System.DateTime)

Time that the alert occurred.

-- TriggerInterval (System.TimeSpan?)

Number of ticks (100ns) before the alert can be raised again.

-- TriggerLevel (System.Double?)

Threshold level that the alert was configured to trigger at.

-- TriggerPeriod (System.TimeSpan?)

Duration the value was above the trigger level.

-- TriggerValue (System.Double?)

The value of the monitored metric that triggered the alert.

-- Uid (System.Int64)

The unique internal identifier of this alert.

Related topics

New-BrokerHypervisorConnection

Parameters

-Uid<Int64>

Gets the hypervisor alert with the specified UID.

Required?	true
Default Value	

Accept Pipeline Input?	false

-HostingServerName<String>

Gets alerts for the specified hosting hypervisor server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets alerts for the specified hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metric<AlertMetric>

Gets alerts for a specified metric.

Valid values are: Cpu, Memory, Network and Disk.

Required?	false

Default Value	
Accept Pipeline Input?	false

-Severity<AlertSeverity>

Gets alerts with the specified severity.

Valid values are: Red and Yellow.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Time<DateTime>

Gets alerts that occurred at a specific time.

You can also use -Filter and relative comparisons; see the examples for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TriggerInterval<TimeSpan>

Gets alerts with a specific trigger interval. This is the interval before the alert is raised again.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TriggerLevel<Double>

Gets alerts with a specific trigger threshold level.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TriggerPeriod<TimeSpan>

Gets alerts with a specific trigger period. This is the duration the threshold level was exceeded for, prior to the alert triggering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TriggerValue<Double>

Gets the value of the monitored metric that triggered the alert.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe objects to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.HypervisorAlert

Get-BrokerHypervisorAlert returns an object for each matching alert.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerHypervisorAlert -HostingServerName TestHyp* -Severity Red
```

Returns all serious (Red) alerts for any hosting server with a name that starts with 'TestHyp'.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerHypervisorAlert -Filter { Metric -eq 'Cpu' -and Time -ge '-1:0' }
```

Returns all CPU usage alerts that occurred in the last hour.

Get-BrokerHypervisorConnection

Sep 10, 2014

Gets hypervisor connections matching the specified criteria.

Syntax

Get-BrokerHypervisorConnection [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerHypervisorConnection [[-Name] <String>] [-HypHypervisorConnectionUid <Guid>] [-IsReady <Boolean>] [-MachineCount <Int32>] [-MaxAbsoluteActiveActions <Int32>] [-MaxAbsoluteNewActionsPerMinute <Int32>] [-MaxAbsolutePvdPowerActions <Int32>] [-MaxPercentageActiveActions <Int32>] [-MaxPvdPowerActionsPercentageOfDesktops <Int32>] [-Metadata <String>] [-PreferredController <String>] [-State <HypervisorConnectionState>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Get-BrokerHypervisorConnection cmdlet gets hypervisor connections matching the specified criteria. If no parameters are specified this cmdlet enumerates all hypervisor connections.

---------- BrokerHypervisorConnection Object

The BrokerHypervisorConnection represents hypervisor connection object. It contains the following properties:

-- Capabilities (System.String[])

The set of capabilities as reported by the hypervisor.

-- HypHypervisorConnectionUid (System.Guid)

The Guid that identifies the hypervisor connection.

-- IsReady (System.Boolean)

Indicates that the connection is ready to be used in the configuration of managed machines.

-- MachineCount (System.Int32)

Count of machines associated with this hypervisor connection.

-- MaxAbsoluteActiveActions (System.Int32?)

Maximum number of active power actions allowed at any one time (defined in the metadata named 'Citrix_Broker_MaxAbsoluteActiveActions' on the hypervisor connection in the Citrix Hosting Service).

-- MaxAbsoluteNewActionsPerMinute (System.Int32?)

Maximum number of new actions that can be fired off to the hypervisor in any one minute (defined in the metadata named 'Citrix_Broker_MaxAbsoluteNewActionsPerMinute' on the hypervisor connection in the Citrix Hosting Service).

-- MaxAbsolutePvdPowerActions (System.Int32?)

Maximum number of active PvD power actions allowed at any one time (defined in the metadata named 'Citrix_Broker_MaxAbsolutePvdPowerActions' on the hypervisor connection in the Citrix Hosting Service).

-- MaxPercentageActiveActions (System.Int32?)

Maximum percentage of machines on the connection that can have active power actions at any one time (defined in the metadata named 'Citrix_Broker_MaxPowerActionsPercentageOfDesktops' on the hypervisor connection in the Citrix Hosting Service).

-- MaxPvdPowerActionsPercentageOfDesktops (System.Int32?)

Maximum percentage of machines on the connection that can be in personal VDisk image preparation mode at any one time (defined in the metadata named 'Citrix_Broker_MaxPvdPowerActionsPercentageOfDesktops' on the hypervisor connection in the Citrix Hosting Service).

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Collection of all the metadata associated to the hypervisor connection.

-- Name (System.String)

The display name of the hypervisor connection.

-- PreferredController (System.String)

The name of the controller which is preferred to be used, when available, to perform all communication to the hypervisor. The name is in DOMAIN\machine form. A preferred controller may have been automatically chosen when the hypervisor connection was created.

-- State (Citrix.Broker.Admin.SDK.HypervisorConnectionState)

The state of the hypervisor connection.

-- Uid (System.Int32)

Unique internal identifier of hypervisor connection.

Related topics

New-BrokerHypervisorConnection

Remove-BrokerHypervisorConnection

Set-BrokerHypervisorConnection

Parameters

-Uid<Int32>

Gets the hypervisor connection with the specified internal id.

Required?	true

Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets hypervisor connections with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypHypervisorConnectionUid<Guid>

Gets hypervisor connections with the specified Guid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsReady<Boolean>

Gets hypervisor connections with the specified value of the IsReady flag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineCount<Int32>

Gets hypervisor connections with the specified machine count.

Required?	false
Default Value	

Accept Pipeline Input?	false

-MaxAbsoluteActiveActions<Int32>

Gets hypervisor connections with the specified MaxAbsoluteActiveActions value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxAbsoluteNewActionsPerMinute<Int32>

Gets hypervisor connections with the specified MaxAbsoluteNewActionsPerMinute value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxAbsolutePvdPowerActions<Int32>

Gets hypervisor connections with the specified MaxAbsolutePvdPowerActions value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxPercentageActiveActions<Int32>

Gets hypervisor connections with the specified MaxPercentageActiveActions value.

Required?	false
Default Value	

Accept Pipeline Input?	false

-MaxPvdPowerActionsPercentageOfDesktops<Int32>

Gets hypervisor connections with the specified MaxPvdPowerActionsPercentageOfDesktops value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-PreferredController<String>

Gets hypervisor connections with the specified preferred controller. Specify the SAM name of the controller.

Required?	false
Default Value	
Accept Pipeline Input?	false

-State<HypervisorConnectionState>

Gets hypervisor connections with the specified connection state. Values can be can be:

o Unavailable - The broker is unable to contact the hypervisor.

o InMaintenanceMode - The hosting server is in maintenance mode.

o On - The broker is in contact with the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None

Return Values

Citrix.Broker.Admin.SDK.HypervisorConnection

Get-BrokerHypervisorConnection returns an object for each matching hypervisor connection.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS> $hvConn = Get-BrokerHypervisorConnection -Name "hvConnectionName"
```

Gets a hypervisor connection by name.

-------------------------- EXAMPLE 2 --------------------------

```
c:\PS> $hvConn = Get-BrokerHypervisorConnection -PreferredController "domainName\controllerName"
```

Gets hypervisor connections by preferred controller.

-------------------------- EXAMPLE 3 --------------------------

```
c:\PS> $machine = Get-BrokerMachine -Uid $machineUid
c:\PS> $hvConn = Get-BrokerHypervisorConnection -Uid $machine.HypervisorConnectionUid
```

Gets hypervisor connection used by a (power managed) machine.

Get-BrokerIcon

Sep 10, 2014

Get stored icons.

Syntax

Get-BrokerIcon -Uid <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerIcon [-Metadata <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Reads a specific icon by Uid, or enumerates icons by passing no Uid.

---------- BrokerIcon Object

The BrokerIcon object represents a single instance of an icon. It contains the following properties:

-- EncodedIconData (System.String)

The Base64 encoded .ICO format of the icon.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Metadata for this command

-- Uid (System.Int32)

The UID of the icon itself.

Related topics

New-BrokerIcon

Remove-BrokerIcon

Parameters

-Uid<Int32>

Gets only the icon specified by unique identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0

Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None Input cannot be piped to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Icon

Returns an Icon object for each enumerated icon.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerIcon
Enumerate all icons.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerIcon -Uid 1
Get the icon with Uid 1.

Get-BrokerImportedFTA

Sep 10, 2014

Gets the imported file type associations.

Syntax

Get-BrokerImportedFTA [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerImportedFTA [[-ExtensionName] <String>] [-ContentType <String>] [-Description <String>] [-DesktopGroupUid <Int32>] [-Edit <String>] [-EditArguments <String>] [-EditExecutableName <String>] [-HandlerName <String>] [-Open <String>] [-OpenArguments <String>] [-OpenExecutableName <String>] [-PerceivedType <String>] [-Print <String>] [-PrintTo <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns the file type associations the system imports from worker machines.

File type association associates a file extension (such as ".txt") with an application (such as Notepad). In a Citrix environment file type associations on a user device can be configured so that when an user clicks on a document it launches the appropriate published application. This is known as "content redirection".

Imported file type associations are different from configured file type associations. Imported file type associations are lists of known file type associations for a given desktop group. Configured file type associations are those that are actually associated with published applications for the purposes of content redirection.

Initially the system is not aware of any extensions, and they must be imported by the Citrix administrator. See the Update-BrokerImportedFTA cmdlet for more information.

After file type extensions are imported, this cmdlet lets the administrator review which file type associations the system is aware of. ImportedFTA objects are also used when configuring content redirection. See the New-BrokerConfiguredFTA cmdlet for more information.

The imported file type associations are grouped according to the desktop group to which they belong, because the system expects all machines in the same desktop group to have the same file type associations. That may not be true, however, across desktop groups.

Note that the ImportedFTA object has several fields that are not currently used. Only those fields that are shared with the ConfiguredFTA object are actually used in some capacity.

---------- BrokerImportedFTA Object

The BrokerImportedFTA object represents a file type association imported from worker machines. It contains the following properties:

-- ContentType (System.String)

Content type of the file, such as "text/plain" or "application/vnd.ms-excel".

-- Description (System.String)

File type description, such as "Test Document", "Microsoft Word Text Document", etc.

-- DesktopGroupUid (System.Int32)

The desktop group this file type belongs to.

-- Edit (System.String)

Edit command with full path to executable: "C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE" /n /dde

-- EditArguments (System.String)

The arguments used for the 'edit' action on files of this type. These are extracted from the full edit command, and may be empty.

-- EditExecutableName (System.String)

The executable name extracted from the Edit property, no path included. This is used for matching with published apps' executable when searching for the list of extensions an application is capable of handling.

-- ExtensionName (System.String)

A single file extension, such as .txt. Unique within the scope of a desktop group.

-- HandlerName (System.String)

File type handler name, e.g. "Word.Document.8" or TXTFILE.

-- Open (System.String)

Open command with full path to executable: "C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE" /n /dde

-- OpenArguments (System.String)

The arguments used for the 'open' action on files of this type. These are extracted from the full open command, and may be empty.

-- OpenExecutableName (System.String)

The executable name extracted from the Open property, no path included. This is used for matching with published apps' executable when searching for the list of extensions an application is capable of handling.

-- PerceivedType (System.String)

Perceived type, such as "text".

-- Print (System.String)

Print command: "C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE" /x /n /dde

-- PrintTo (System.String)

PrintTo command: "C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE" /n /dde

-- Uid (System.Int32)

Unique internal identifier of imported file type association.

Related topics

New-BrokerConfiguredFTA

Remove-BrokerImportedFTA

Update-BrokerImportedFTA

Parameters

-Uid<Int32>

Gets only the imported file type associations with the specified unique identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ExtensionName<String>

Gets only the imported file type associations with the specified extension name. For example, ".txt" or ".png".

Required?	false
Default Value	
Accept Pipeline Input?	false

-ContentType<String>

Gets only the imported file type associations with the specified content type (as listed in the Registry). For example, "application/msword".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets only the imported file type associations with the specified description (as listed in the Registry). For example, "Text Document" or "Microsoft Word text document".

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets only the file type associations imported from a worker machine belonging to the specified desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Edit<String>

Gets only the imported file type associations with the specified Edit command, that includes both the executable name and path, and any arguments to that executable.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EditArguments<String>

Gets only the imported file type associations with the specified arguments to the Edit command.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EditExecutableName<String>

Gets only the imported file type associations with the specified executable for the Edit command.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HandlerName<String>

Gets only the imported file type associations with the specified handler name (as listed in the Registry). For example, "TXTFILE" or "Word.Document.8".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Open<String>

Gets only the imported file type associations with the specified Open command, that includes both the executable name and path, and any arguments to that executable.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OpenArguments<String>

Gets only the imported file type associations with the specified arguments to the Open command.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OpenExecutableName<String>

Gets only the imported file type associations with the specified executable for the Open command.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PerceivedType<String>

Gets only the imported file type associations with the specified perceived type (as listed in the Registry). For example, "document".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Print<String>

Gets only the imported file type associations with the specified Print command.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PrintTo<String>

Gets only the imported file type associations with the specified PrintTo command.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None This cmdlet does not accept any input from the pipeline.

Return Values

Citrix.Broker.Admin.SDK.ImportedFTA

One or more ImportedFTA objects are returned as output.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerImportedFTA
Invoking this cmdlet with no arguments simply returns all of the imported file type association objects. By default, only the first 250 objects are returned. See the -MaxRecordCount and -Skip parameters for information about modifying this.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerImportedFTA -ExtensionName ".txt"
Retrieves all imported file type associations that have the extension ".txt". Note that because imported file type associations are per-desktop group, multiple instances may be returned.

Get-BrokerInstalledDbVersion

Sep 10, 2014

Gets a list of all available database schema versions for the Broker Service.

Syntax

```
Get-BrokerInstalledDbVersion [-Upgrade] [-Downgrade] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets the current version number of the Citrix Broker Service database schema when called with no parameters.

When called with the -Upgrade parameter, gets the service schema version numbers to which an upgrade could be performed.

When called with the -Downgrade parameter, gets the service schema version numbers to which a downgrade could be performed.

The SQL scripts to perform schema upgrades and downgrades can be obtained using the Get-BrokerDBVersionChangeScript cmdlet. Citrix recommends that where possible service schema upgrades are performed using Studio rather than manually via the SDK.

Only one of the -Upgrade or -Downgrade parameters may be supplied at once.

Related topics

Get-BrokerDBVersionChangeScript

Get-BrokerDBSchema

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

System.Version

Get-BrokerInstalledDBVersion returns database schema version numbers as requested.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Broker Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-BrokerInstalledDBVersion
```

Gets the current Citrix Broker Service database schema version number.

---------- EXAMPLE 2 ----------

```
C:\PS>Get-BrokerInstalledDBVersion -Upgrade
```

Get the versions of the Broker Service database schema for which upgrade scripts are supplied.

Get-BrokerLease

Sep 10, 2014

Gets stored leases.

Syntax

Get-BrokerLease [-Uid] <Int64> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerLease [[-Key] <String>] [-Expiration <DateTime>] [-LastModified <DateTime>] [-LeaseType <BrokerLeaseType>] [-OwnerSAMName <String>] [-OwnerSID <String>] [-OwnerUPN <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets leases filtered by specific Uid or Owner information.

---------- BrokerLease Object

The BrokerLease object represents a single instance of a lease. It contains the following properties:

-- Expiration (System.DateTime)

The expiration time of the lease.

-- Key (System.String)

The SHA1 representation of the lease key.

-- LastModified (System.DateTime)

The modification time of the lease.

-- LeaseType (Citrix.Broker.Admin.SDK.BrokerLeaseType)

The type of lease.

-- OwnerSAMName (System.String)

The SAM name of the user associated with the lease.

-- OwnerSID (System.String)

The SID of the user associated with the lease.

-- OwnerUPN (System.String)

The UPN of the user associated with the lease.

-- Uid (System.Int64)

The UID of the lease itself.

-- Value (System.String)

The serialized lease data in XML.

Related topics

Remove-BrokerLease

Update-BrokerLocalLeaseCache

Parameters

-Uid<Int64>

Gets only the lease specified by unique identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Key<String>

Gets only the leases matching the specified lease key pattern.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Expiration<DateTime>

Gets only the leases matching the specified expiration date and time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastModified<DateTime>

Gets only the leases matching the specified modified date and time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LeaseType<BrokerLeaseType>

Gets only leases of a specific type. Possible values Enumeration, Launch.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OwnerSAMName<String>

Gets only the leases associated with the specified Domain\User.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OwnerSID<String>

Gets only the leases associated with the specified user SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OwnerUPN<String>

Gets only the leases associated with the specified user UPN.

Required?	false

Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if

no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None Input cannot be piped to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Lease

Returns an Lease object for each enumerated lease.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $lease = Get-BrokerLease -Uid 1
```

Gets the lease with internal Uid 1.

---------- EXAMPLE 2 ----------

```
C:\PS> $leases = Get-BrokerLease -OwnerSAMName Domain\User
```

Gets the leases associated with the specified user.

Get-BrokerMachine

Sep 10, 2014

Gets machines belonging to this site.

Syntax

Get-BrokerMachine [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerMachine [[-MachineName] <String>] [-AgentVersion <String>] [-AllocationType <AllocationType>] [-ApplicationInUse <String>] [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-AssociatedUserFullName <String>] [-AssociatedUserName <String>] [-AssociatedUserSID <String>] [-AssociatedUserUPN <String>] [-BrowserName <String>] [-CatalogName <String>] [-CatalogUid <Int32>] [-CatalogUUID <Guid>] [-ColorDepth <ColorDepth>] [-ControllerDNSName <String>] [-DeliveryType <DeliveryType>] [-Description <String>] [-DesktopCondition <String>] [-DesktopGroupName <String>] [-DesktopGroupUid <Int32>] [-DesktopGroupUUID <Guid>] [-DesktopKind <DesktopKind>] [-DesktopUid <Int32>] [-DNSName <String>] [-FaultState <MachineFaultState>] [-FunctionalLevel <FunctionalLevel>] [-HostedMachineId <String>] [-HostedMachineName <String>] [-HostingServerName <String>] [-HypervisorConnectionName <String>] [-HypervisorConnectionUid <Int32>] [-HypHypervisorConnectionUid <Guid>] [-IconUid <Int32>] [-ImageOutOfDate <Boolean>] [-InMaintenanceMode <Boolean>] [-IPAddress <String>] [-IsAssigned <Boolean>] [-IsPhysical <Boolean>] [-LastConnectionFailure <ConnectionFailureReason>] [-LastConnectionTime <DateTime>] [-LastConnectionUser <String>] [-LastDeregistrationReason <DeregistrationReason>] [-LastDeregistrationTime <DateTime>] [-LastErrorReason <String>] [-LastErrorTime <DateTime>] [-LastHostingUpdateTime <DateTime>] [-LastPvdErrorReason <String>] [-LastPvdErrorTime <DateTime>] [-LoadIndex <Int32>] [-MachineInternalState <MachineInternalState>] [-Metadata <String>] [-OSType <String>] [-OSVersion <String>] [-PersistUserChanges <PersistUserChanges>] [-PowerActionPending <Boolean>] [-PowerState <PowerState>] [-ProvisioningType <ProvisioningType>] [-PublishedApplication <String>] [-PublishedName <String>] [-PvdEstimatedCompletionTime <DateTime>] [-PvdPercentDone <Int32>] [-PvdStage <PvdStage>] [-PvdUpdateStartTime <DateTime>] [-RegistrationState <RegistrationState>] [-ScheduledReboot <ScheduledReboot>] [-SecureIcaRequired <Boolean>] [-SessionAutonomouslyBrokered <Boolean>] [-SessionClientAddress <String>] [-SessionClientName <String>] [-SessionClientVersion <String>] [-SessionConnectedViaHostName <String>] [-SessionConnectedViaIP <String>] [-SessionCount <Int32>] [-SessionDeviceId <String>] [-SessionHardwareId <String>] [-SessionHidden <Boolean>] [-SessionKey <Guid>] [-SessionLaunchedViaHostName <String>] [-SessionLaunchedViaIP <String>] [-SessionProtocol <String>] [-SessionSecureIcaActive <Boolean>] [-SessionsEstablished <Int32>] [-SessionSmartAccessTag <String>] [-SessionsPending <Int32>] [-SessionStartTime <DateTime>] [-SessionState <SessionState>] [-SessionStateChangeTime <DateTime>] [-SessionSupport <SessionSupport>] [-SessionType <SessionType>] [-SessionUid <Int64>] [-SessionUserName <String>] [-SessionUserSID <String>] [-SID <String>] [-SummaryState <DesktopSummaryState>] [-SupportedPowerActions <String[]>] [-Tag <String>] [-UUID <Guid>] [-VMToolsState <VMToolsState>] [-WillShutdownAfterUse <Boolean>] [-WindowsConnectionSetting <WindowsConnectionSetting>] [-AssignedUserSID <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieves machines matching the specified criteria. If no parameters are specified, this cmdlet enumerates all machines.

Get-BrokerMachine returns objects that combine machine configuration and state information.

For single-session machines, session information is displayed if present. If "fast user switching" is enabled, more than one session may be present on single-session machines. Because this cmdlet returns information only for a single session, if two sessions are present it will return information about the brokered session (rather than, for example, an unbrokered direct RDP session). If there is no session running, session-related fields return $null.

For multi-session machines, no session information about single sessions is displayed by this cmdlet, and so are always $null. Get-BrokerSession can be used to get information about sessions on both multi-session and single-session machines.

To count machines, rather than retrieve full details of each machine, use Group-BrokerMachine instead.

See about_Broker_Filtering for information about advanced filtering options, and about_Broker_Machines for background information about machines.

---------- BrokerMachine Object

The machine object returned represents a physical or virtual machine, which has been configured in the site.

-- AgentVersion (System.String)

Version of the Citrix Virtual Delivery Agent (VDA) installed on the machine.

-- AllocationType (Citrix.Broker.Admin.SDK.AllocationType)

Describes how the machine is allocated to the user, can be Permanent or Random.

-- ApplicationsInUse (System.String[])

List of applications in use on the machine (in the form of browser name).

-- AssignedClientName (System.String)

The name of the endpoint client device that the machine has been assigned to.

-- AssignedIPAddress (System.String)

The IP address of the endpoint client device that the machine has been assigned to.

-- AssociatedUserFullNames (System.String[])

Full names of the users that have been associated with the machine (usually in the form "Firstname Lastname").

Associated users are the current user(s) for shared machines and the assigned users for private machines.

-- AssociatedUserNames (System.String[])

Usernames of the users that have been associated with the machine (in the form "domain\user").

Associated users are the current user(s) for shared machines and the assigned users for private machines.

-- AssociatedUserSIDs (System.String[])

The SIDs of the users that have been associated with the machine.

Associated users are the current user(s) for shared machines and the assigned users for private machines.

-- AssociatedUserUPNs (System.String[])

The User Principal Names of the users associated with the machine (in the form user@domain).

Associated users are the current user(s) for shared machines and the assigned users for private machines.

-- BrowserName (System.String)

Site-wide unique name identifying associated desktop to other components (for example StoreFront). This is typically non-null only for machines backing assigned private desktops.

-- Capabilities (System.String[])

List of the capabilities that the machine supports. Valid capabilities are:

o MultiSession: Indicates an RDS- (Terminal Services-) based machine, which supports multiple active sessions from different users.

o CBP1_5: Indicates the machine uses the CBP 1.5 protocol for communication.

-- CatalogName (System.String)

Name of the catalog the machine is a member of.

-- CatalogUid (System.Int32)

UID of the catalog the machine is a member of.

-- CatalogUUID (System.Guid)

UUID of the catalog the machine is a member of.

-- ColorDepth (Citrix.Broker.Admin.SDK.ColorDepth?)

The color depth setting configured on the machine, possible values are:

$null, FourBit, EightBit, SixteenBit, and TwentyFourBit.

-- ControllerDNSName (System.String)

The DNS host name of the controller that the machine is registered to.

-- DeliveryType (Citrix.Broker.Admin.SDK.DeliveryType?)

Denotes whether the machine delivers desktops only, apps only or both.

-- Description (System.String)

Description of the machine.

-- DesktopConditions (System.String[])

List of outstanding desktop conditions for the machine.

-- DesktopGroupName (System.String)

Name of the desktop group the machine is a member of.

-- DesktopGroupUid (System.Int32?)

UID of the desktop group the machine is a member of.

-- DesktopGroupUUID (System.Guid?)

UUID of the desktop group the machine is a member of.

-- DesktopKind (Citrix.Broker.Admin.SDK.DesktopKind?)

Deprecated.

Denotes whether the machine is private or shared. Use AllocationType instead.

-- DesktopUid (System.Int32?)

The UID of the associated desktop object.

-- DNSName (System.String)

The DNS host name of the machine.

-- FaultState (Citrix.Broker.Admin.SDK.MachineFaultState)

Summary state of any current fault state of the machine. Can be one of the following:

o None - No fault; machine is healthy.

o FailedToStart - Last power-on operation for machine failed.

o StuckOnBoot - Machine does not seem to have booted following power on.

o Unregistered - Machine has failed to register within expected period, or its registration has been rejected.

o MaxCapacity - Machine is reporting itself at maximum capacity.

-- FunctionalLevel (Citrix.Broker.Admin.SDK.FunctionalLevel?)

Functional level of the machine, if known.

-- HostedMachineId (System.String)

Unique ID within the hosting unit of the target managed machine.

-- HostedMachineName (System.String)

The friendly name of a hosted machine as used by its hypervisor. This is not necessarily the DNS name of the machine.

-- HostingServerName (System.String)

DNS name of the hypervisor that is hosting the machine if managed.

-- HypervisorConnectionName (System.String)

The name of the hypervisor connection that the machine has been assigned to, if managed.

-- HypervisorConnectionUid (System.Int32?)

The UID of the hypervisor connection that the machine's hosting server is accessed through.

-- HypHypervisorConnectionUid (System.Guid?)

The UUID of the hypervisor connection that the machine's hosting server is accessed through

-- IconUid (System.Int32?)

The UID of the machine's icon that is displayed in StoreFront.

-- ImageOutOfDate (System.Boolean?)

Denotes if the VM image for a hosted machine is out of date.

-- InMaintenanceMode (System.Boolean)

Denotes if the machine is in maintenance mode.

-- IPAddress (System.String)

The IP address of the machine.

-- IsAssigned (System.Boolean)

Denotes whether a private desktop has been assigned to a user/users, or a client name/address. Users can be assigned explicitly or by assigning on first use of the machine.

-- IsPhysical (System.Boolean)

This value is true if the machine is physical (ie not power managed by the Citrix Broker service, and false otherwise.

-- LastConnectionFailure (Citrix.Broker.Admin.SDK.ConnectionFailureReason)

The reason for the last failed connection between a client and the machine.

-- LastConnectionTime (System.DateTime?)

Time of the last detected connection attempt that either failed or succeeded.

-- LastConnectionUser (System.String)

The SAM name (in the form DOMAIN\user) of the user that last attempted a connection with the machine. If the SAM name is not available, the SID is used.

-- LastDeregistrationReason (Citrix.Broker.Admin.SDK.DeregistrationReason?)

The reason for the last deregistration of the machine with the broker. Possible values are:

AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog,

FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

-- LastDeregistrationTime (System.DateTime?)

Time of the last deregistration of the machine from the controller.

-- LastErrorReason (System.String)

The reason for the last error detected in the machine.

-- LastErrorTime (System.DateTime?)

The time of the last detected error.

-- LastHostingUpdateTime (System.DateTime?)

Time of last update to any hosting data (such as power states) for this machine reported by the hypervisor connection.

-- LastPvdErrorReason (System.String)

The error text from the most recent failure of the Personal vDisk preparation process for this machine (if any).

-- LastPvdErrorTime (System.DateTime?)

The time of the most recent failure of the Personal vDisk preparation process for this machine (if any).

-- LoadIndex (System.Int32?)

Gives current effective load index for multi-session machines.

-- LoadIndexes (System.String[])

Gives the last reported individual load indexes that were used in the calculation of the LoadIndex value. Note that the LoadIndex value may have been subsequently adjusted due to session brokering operations. This value is only set for multi-session machines.

-- MachineInternalState (Citrix.Broker.Admin.SDK.MachineInternalState)

The internal state of the machine; reported while the machine is registered to a controller, plus some private Citrix Broker Service states while the machine is not registered.

-- MachineName (System.String)

DNS host name of the machine.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Any metadata that is associated with the machine.

-- OSType (System.String)

A string that can be used to identify the operating system that is running on the machine.

-- OSVersion (System.String)

A string that can be used to identify the version of the operating system running on the machine, if known.

-- PersistUserChanges (Citrix.Broker.Admin.SDK.PersistUserChanges)

Describes if and how user changes are persisted. Possible values are:

o OnLocal - Persist the user changes on the local disk of the machine.

o Discard - Discard user changes.

o OnPvd - Persist user changes on the Citrix Personal vDisk.

-- PowerActionPending (System.Boolean)

Indicates if there are any pending power actions for the machine.

-- PowerState (Citrix.Broker.Admin.SDK.PowerState)

The current power state of the machine. Possible values are: Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, resuming.

-- ProvisioningType (Citrix.Broker.Admin.SDK.ProvisioningType)

Describes how the machine was provisioned, possible values are:

o Manual: No automated provisioning.

o PVS: Machine provisioned by PVS (may be physical, blade, VM,...)

o MCS: Machine provisioned by MCS (machine must be VM)

-- PublishedApplications (System.String[])

List of applications published by the machine (displayed as browser names).

-- PublishedName (System.String)

The name of the machine that is displayed in StoreFront, if the machine has been published.

-- PvdEstimatedCompletionTime (System.DateTime?)

If preparation of the Personal vDisk is currently in progress for this machine, this reports an estimation of the time at which the process will be complete.

-- PvdPercentDone (System.Int32?)

If preparation of the Personal vDisk is currently in progress for this machine, this reports how far the process has got as a percentage. This value will be zero if preparation is not in progress.

-- PvdStage (Citrix.Broker.Admin.SDK.PvdStage)

For a machine supporting Personal vDisk technology (PvD), indicates the stage of the PvD image preparation.

-- PvdUpdateStartTime (System.DateTime?)

If preparation of the Personal vDisk is currently in progress for this machine, this reports when the update process began.

-- RegistrationState (Citrix.Broker.Admin.SDK.RegistrationState)

Indicates the registration state of the machine. Possible values are: Unregistered, Initializing, Registered, AgentError.

-- ScheduledReboot (Citrix.Broker.Admin.SDK.ScheduledReboot)

Indicates the state of any scheduled reboot operation for a machine. Possible values:

o None: No reboot is scheduled.

o Pending: Machine is awaiting reboot but is available for use.

o Draining: Machine is awaiting reboot and is unavailable for new sessions; reconnections to existing connections are still allowed, however.

o InProgress: Machine is actively undergoing a scheduled reboot. o Natural: Natural reboot in progress. Machine is awaiting a restart.

-- SecureIcaRequired (System.Boolean?)

Flag indicating whether SecureICA is required or not when starting a session on the machine.

-- SessionAutonomouslyBrokered (System.Boolean?)

Session property indicating if the current session is an HDX session established by direct connection without being brokered.

Session properties are always null for multi-session machines.

-- SessionClientAddress (System.String)

Session property indicating the IP address of the client connected to the machine.

Session properties are always null for multi-session machines.

-- SessionClientName (System.String)

Session property indicating the host name of the client connected to the machine.

Session properties are always null for multi-session machines.

-- SessionClientVersion (System.String)

Session property indicating the version of the Citrix Receiver on the connected client.

Session properties are always null for multi-session machines.

-- SessionConnectedViaHostName (System.String)

Session property indicating the host name of the connection gateway, router or client.

Session properties are always null for multi-session machines.

-- SessionConnectedViaIP (System.String)

Session property indicating the IP address of the connection gateway, router or client.

Session properties are always null for multi-session machines.

-- SessionCount (System.Int32)

Count of number of sessions on the machine.

-- SessionDeviceId (System.String)

Session property indicating a unique identifier for the client device that has most recently been associated with the current session.

Session properties are always null for multi-session machines.

-- SessionHardwareId (System.String)

Session property indicating a unique identifier for the client hardware that has been most recently associated with the current session.

Session properties are always null for multi-session machines.

-- SessionHidden (System.Boolean?)

Session property that indicates if a session is hidden.

Session properties are always null for multi-session machines.

-- SessionKey (System.Guid?)

Session property indicating the key of the current session.

Session properties are always null for multi-session machines.

-- SessionLaunchedViaHostName (System.String)

Session property that denotes the host name of the StoreFront server used to launch the current brokered session.

Session properties are always null for multi-session machines.

-- SessionLaunchedViaIP (System.String)

Session property that denotes the IP address of the StoreFront server used to launch the current brokered session.

Session properties are always null for multi-session machines.

-- SessionProtocol (System.String)

Session property that denotes the protocol that the current session is using, can be either HDX, RDP or Console. Console sessions on XenDesktop 5 VDAs appear with a blank protocol.

Session properties are always null for multi-session machines.

-- SessionSecureIcaActive (System.Boolean?)

Session property that indicates whether SecureICA is active on the current session or not.

Session properties are always null for multi-session machines.

-- SessionsEstablished (System.Int32)

Number of established sessions on this machine. For multi-session machines this excludes established sessions which have not yet completed their logon processing.

-- SessionSmartAccessTags (System.String[])

Session property that indicates the Smart Access tags for the current session.

Session properties are always null on multi-session machines.

-- SessionsPending (System.Int32)

Number of pending (brokered but not yet established) sessions on this machine. For multi-session machines this also includes established sessions which have not yet completed their logon processing.

-- SessionStartTime (System.DateTime?)

Session property that indicates the start time of the current session.

Session properties are always null on multi-session machines.

-- SessionState (Citrix.Broker.Admin.SDK.SessionState?)

Session property indicating the state of the current session, possible values are:

Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession and Unknown. Session properties are always null for multi-session machines.

-- SessionStateChangeTime (System.DateTime?)

Session property indicating the time of the last state change of the current session.

Session properties are always null for multi-session machines.

-- SessionSupport (Citrix.Broker.Admin.SDK.SessionSupport)

Indicates the session support of the machine.

Possible values:

o SingleSession: Single-session only machine.

o MultiSession: Multi-session capable machine.

-- SessionType (Citrix.Broker.Admin.SDK.SessionType?)

Session property indicating the type of the current session.

Session properties are always null for multi-session machines.

-- SessionUid (System.Int64?)

Session property indicating the UID of the current session.

Session properties are always null for multi-session machines.

-- SessionUserName (System.String)

Session property indicates the name of the current session's user (in the form DOMAIN\user).

Session properties are always null for multi-session machines.

-- SessionUserSID (System.String)

Session property indicates the SID of the current session's user.

Session properties are always null for multi-session machines.

-- SID (System.String)

The SID of the machine.

-- SummaryState (Citrix.Broker.Admin.SDK.DesktopSummaryState)

Indicates the overall state of the desktop associated with the machine. The overall state is a result of other more specific states such as session state, registration state and power state. Possible values: Off, Unregistered, Available, Disconnected, InUse, Preparing.

-- SupportedPowerActions (System.String[])

A list of power actions supported by this machine.

-- Tags (System.String[])

A list of tags for the machine.

-- Uid (System.Int32)

UID of the machine object.

-- UUID (System.Guid)

UUID of the machine object.

-- VMToolsState (Citrix.Broker.Admin.SDK.VMToolsState)

State of the hypervisor tools present on the VM (if any).

Possible values are:

NotPresent, Unknown, NotStarted, Running.

-- WillShutdownAfterUse (System.Boolean)

Flag indicating if this machine is tainted and will be shut down after all sessions on the machine have ended. This flag is only ever true on power-managed, single-session machines.

Note: The machine will not shut down if it is in maintenance mode; it will shut down only after it is taken out of maintenance mode.

-- WindowsConnectionSetting (Citrix.Broker.Admin.SDK.WindowsConnectionSetting?)

The logon mode reported by Windows itself (multi-session machines only). For single-session machines the value is always hardwired to LogonEnabled.

Possible values are:

LogonEnabled, Draining, DrainingUntilRestart and LogonDisabled.

Related topics

Group-BrokerMachine

Parameters

-Uid<Int32>

Gets a machine with a specific UID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets machines with a specific machine name (in the form domain\machine).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AgentVersion<String>

Gets machines with a specific Citrix Virtual Delivery Agent version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AllocationType<AllocationType>

Gets machines from catalogs with the specified allocation type.

Required?	false

Default Value	
Accept Pipeline Input?	false

-ApplicationInUse<String>

Gets machines running a specified published application (identified by browser name).

String comparisons are case-insensitive.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedClientName<String>

Gets machines that have been assigned to the specific client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedIPAddress<String>

Gets machines that have been assigned to the specific IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserFullName<String>

Gets machines with an associated user identified by their full name (usually 'first-name last-name').

Associated users are all current users of a desktop, plus the assigned users for private desktops.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AssociatedUserName<String>

Gets machines with an associated user identified by their user name (in the form 'domain\user').

Associated users are all current users of a desktop, plus the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserSID<String>

Gets machines with an associated user identified by their Windows SID.

Associated users are all current users of a desktop, plus the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserUPN<String>

Gets machines with an associated user identified by their User Principle Name (in the form 'user@domain').

Associated users are all current users of a desktop, plus the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrowserName<String>

Gets assigned machines backing desktop resources that have browser names matching the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogName<String>

Gets machines from the catalog with the specific name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogUid<Int32>

Gets machines from the catalog with the specific UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogUUID<Guid>

Gets machines from the catalog with the specific UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Gets machines configured with a specific color depth.

Valid values are FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ControllerDNSName<String>

Gets machines with a specific DNS name of the controller they are registered with.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeliveryType<DeliveryType>

Gets machines of a particular delivery type.

Valid values are AppsOnly, DesktopsOnly, DesktopsAndApps

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets machines with a specific description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopCondition<String>

Gets machines with an outstanding desktop condition.

Valid values are:

o CPU: Indicates the machine has high CPU usage

o ICALatency: Indicates the network latency is high

o UPMLogonTime: Indicates that the profile load time was high

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets machines from a desktop group with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets machines from a desktop group with a specific UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUUID<Guid>

Gets machines from a desktop group with a specific UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopKind<DesktopKind>

Deprecated: Use AllocationType parameter.

Gets machines of a particular kind.

Valid values are Private, Shared.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopUid<Int32>

Gets the machine that corresponds to the desktop with the specific UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets machines with the specific DNS name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-FaultState<MachineFaultState>

Gets machines currently in the specified fault state.

Required?	false
Default Value	
Accept Pipeline Input?	false

-FunctionalLevel<FunctionalLevel>

Gets machines with a specific FunctionalLevel.

Valid values are L5, L7, L7_6

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineId<String>

Gets machines with the specific machine ID known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets machines with the specific machine name known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostingServerName<String>

Gets machines by the name of the hosting hypervisor server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionName<String>

Gets machines with the specific name of the hypervisor connection hosting them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets machines with the specific UID of the hypervisor connection hosting them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypHypervisorConnectionUid<Guid>

Gets machines with the specific UUID of the hypervisor connection hosting them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Gets machines by configured icon. Note that machines with a null IconUid use the icon of the desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ImageOutOfDate<Boolean>

Gets machines depending on whether their disk image is out of date or not (for machines provisioned using MCS only).

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Gets machines by whether they are in maintenance mode or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IPAddress<String>

Gets machines with a specific IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsAssigned<Boolean>

Gets machines according to whether they are assigned or not. Machines may be assigned to one or more users or groups, a client IP address or a client endpoint name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsPhysical<Boolean>

Gets machines according to whether they can be power managed by XenDesktop or not.

Required?	false

Default Value	
Accept Pipeline Input?	false

-LastConnectionFailure<ConnectionFailureReason>

Gets machines with a specific reason for the last recorded connection failure. This value is None if the last connection was successful or if there has been no attempt to connect to the desktop yet.

Valid values are None, SessionPreparation, RegistrationTimeout, ConnectionTimeout, Licensing, Ticketing, and Other.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastConnectionTime<DateTime>

Gets machines on which a user session connection occurred at a specific time. This is the time at which the broker detected that the connection attempt either succeeded or failed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastConnectionUser<String>

Gets machines where a specific user name last attempted a connection (in the form 'domain\user').

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationReason<DeregistrationReason>

Gets machines whose broker last recorded a specific deregistration reason.

Valid values are $null, AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationTime<DateTime>

Gets machines by the time that they were last deregistered.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastErrorReason<String>

Gets machines with the specified last error reason.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastErrorTime<DateTime>

Gets machines with the specified last error time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastHostingUpdateTime<DateTime>

Gets machines with a specific time that the hosting information was last updated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastPvdErrorReason<String>

Gets machines with the specified last Personal vDisk preparation error reason.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastPvdErrorTime<DateTime>

Gets machines with the specified last Personal vDisk preparation error time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoadIndex<Int32>

Gets machines by their current load index.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineInternalState<MachineInternalState>

Gets machines with the specified internal state.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets machines by the type of operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSVersion<String>

Gets machines by the version of the operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PersistUserChanges<PersistUserChanges>

Gets machines by the location where the user changes are persisted.

o OnLocal - User changes are persisted locally.

o Discard - User changes are discarded.

o OnPvd - User changes are persisted on the Pvd.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerActionPending<Boolean>

Gets machines depending on whether a power action is pending or not.

Valid values are $true or $false.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerState<PowerState>

Gets machines with a specific power state.

Valid values are Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningType<ProvisioningType>

Gets machines that are in a catalog with a particular provisioning type. Values can be:

o Manual - No provisioning.

o PVS - Machine provisioned by PVS (machine may be physical, blade, VM,...).

o MCS - Machine provisioned by MCS (machine must be VM).

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedApplication<String>

Gets machines with a specific application published to them (identified by its browser name).

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Gets desktops with a specific published name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdEstimatedCompletionTime<DateTime>

If preparation of the Personal vDisk is currently in progress for this machine, this reports an estimation of the time at which the process will be complete.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdPercentDone<Int32>

Gets machines a specific percentage through the Personal vDisk preparation process.

This property is typically used with advanced filtering; see about_Broker_Filtering.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdStage<PvdStage>

Gets machines at a specific personal vDisk stage.

Valid values are None, Requested, Starting, Working and Failed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdUpdateStartTime<DateTime>

If preparation of the Personal vDisk is currently in progress for this machine, this reports when the update process began.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RegistrationState<RegistrationState>

Gets machines in a specific registration state.

Valid values are Unregistered, Initializing, Registered, and AgentError.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScheduledReboot<ScheduledReboot>

Gets machines according to their current status with respect to any scheduled reboots (for either scheduled desktop group reboots or image rollout purposes). Valid values are:

o None - No reboot currently scheduled.

o Pending - Reboot scheduled but machine still available for use.

o Draining - Reboot scheduled. New logons are disabled, but reconnections to existing sessions are allowed.

o InProgress - Machine is actively being rebooted.

o Natural - Natural reboot in progress. Machine is awaiting a restart.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Gets machines configured with a particular SecureIcaRequired setting. Note that the machine setting of $null indicates that the desktop group value is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionAutonomouslyBrokered<Boolean>

Gets machines according to whether their current session is autonomously brokered or not. Autonomously brokered sessions are HDX sessions established by direct connection without being brokered.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionClientAddress<String>

Gets machines with a specific client IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionClientName<String>

Gets machines with a specific client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionClientVersion<String>

Gets machines with a specific client version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionConnectedViaHostName<String>

Gets machines with a specific incoming connection host name. This is usually a proxy or Citrix Access Gateway server.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionConnectedViaIP<String>

Gets machines with a specific incoming connection IP address.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionCount<Int32>

Gets machines according to the total number of both pending and established user sessions on the machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionDeviceId<String>

Gets machines with a specific client device ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionHardwareId<String>

Gets machines with a specific client hardware ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionHidden<Boolean>

Gets machines depending on whether their sessions are hidden or not. Hidden sessions are treated as though they do not exist when launching sessions using XenDesktop; a hidden session cannot be reconnected to, but a new session may be launched using the same entitlement.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionKey<Guid>

Gets machine running the session with a specified unique key.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionLaunchedViaHostName<String>

Gets machines with a specific host name of the StoreFront server from which the user launched the session.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionLaunchedViaIP<String>

Gets machines with a specific IP address of the StoreFront server from which the user launched the session.

Session properties are always null for multi-session machines.

Required?	false
Default Value	

Accept Pipeline Input?	false

-SessionProtocol<String>

Gets machines with connections using a specific protocol, for example HDX, RDP, or Console.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSecureIcaActive<Boolean>

Gets machines depending on whether the current session uses SecureICA or not.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionsEstablished<Int32>

Gets machines according to the number of established user sessions present on the machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSmartAccessTag<String>

Gets machines where the session has the specific SmartAccess tag.

Session properties are always null for multi-session machines.

Required?	false
Default Value	

Accept Pipeline Input?	false

-SessionsPending<Int32>

Get machines according to the number of pending user sessions for the machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionStartTime<DateTime>

Gets machines with a specific session start time.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionState<SessionState>

Gets machines with a specific session state.

Valid values are $null, Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession, and Unknown.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionStateChangeTime<DateTime>

Gets machines whose sessions last changed state at a specific time.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSupport<SessionSupport>

Gets machines that have the specified session capability. Values can be:

o SingleSession - Single-session only machine.

o MultiSession - Multi-session capable machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionType<SessionType>

Gets machines with a specific session state.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUid<Int64>

Gets machines with a specific session UID ($null for no session).

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUserName<String>

Gets machines with a specific user name for the current session (in the form 'domain\user').

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUserSID<String>

Gets machines with a specific SID of the current session user.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SID<String>

Gets machines with a specific machine SID.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SummaryState<DesktopSummaryState>

Gets machines with a specific summary state.

Valid values are Off, Unregistered, Available, Disconnected, and InUse.

Required?	false

Default Value	
Accept Pipeline Input?	false

-SupportedPowerActions<String[]>

A list of power actions supported by this machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Tag<String>

Gets machines where the session has the given SmartAccess tag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UUID<Guid>

Gets machines with the specified value of UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-VMToolsState<VMToolsState>

Gets machines with a specific VM tools state.

Valid values are NotPresent, Unknown, NotStarted, and Running.

Required?	false
Default Value	

Accept Pipeline Input?	false

-WillShutdownAfterUse<Boolean>

Gets machines depending on whether they shut down after use or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WindowsConnectionSetting<WindowsConnectionSetting>

Gets machines according to their current Windows connection setting (logon mode). Valid values are:

o LogonEnabled - All logons are enabled.

o Draining - New logons are disabled, but reconnections to existing sessions are allowed.

o DrainingUntilRestart - Same as Draining, but setting reverts to LogonEnabled when machine next restarts.

o LogonDisabled - All logons and reconnections are disabled.

This is a Windows setting and is not controlled by XenDesktop. It applies only to multi-session machines; for single-session machines its value is always LogonEnabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedUserSID<String>

Gets machines with the specific SID of the user to whom the desktop is assigned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Machine

Get-BrokerMachine returns an object for each matching desktop.

Notes

It is generally better to compare dates and times using -Filter and relative comparisons. See about_Broker_Filtering and the examples in this topic for more information.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerMachine -PowerState Suspended
C:\PS> Get-BrokerMachine -Filter { PowerState -eq 'Suspended' }
These commands return all suspended machines. The second form uses advanced filtering (see about_Broker_Filtering).

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerMachine -DNSName '*.mydomain.mycompany.com'
This command returns all machines belonging to the DNS domain mydomain.mycompany.com.

---------- EXAMPLE 3 ----------

C:\PS> Get-BrokerMachine -Filter { RegistrationState -eq 'Registered' -and HypervisorConnectionUid -eq 5 }
This command returns all registered machines running on the specified hypervisor connection.

---------- EXAMPLE 4 ----------

C:\PS> Get-BrokerMachine -MachineName 'MyDomain\X*' | Remove-BrokerDesktopGroup -DesktopGroup 2
This command finds all of the machines in MyDomain with names beginning with X and removes them from the specified desktop group.

---------- EXAMPLE 5 ----------

C:\PS> Get-BrokerMachine -Filter { DesktopGroupUid -ne $null }
This command gets all desktops in a site. Use this instead of the deprecated Get-BrokerDesktop command.

Get-BrokerMachineCommand

Sep 10, 2014

Get the list of commands queued for delivery to a desktop.

Syntax

```
Get-BrokerMachineCommand -Uid <Int64> [-Property <String[]>] [-AdminAddress <String>]
[<CommonParameters>]

Get-BrokerMachineCommand [-Category <String>] [-CommandName <String>] [-CompletionTime
<DateTime>] [-MachineName <String>] [-MachineUid <Int32>] [-Metadata <String>] [-RequestTime
<DateTime>] [-SendDeadline <TimeSpan>] [-SendDeadlineTime <DateTime>] [-SendTrigger
<MachineCommandTrigger>] [-SessionUid <Int64>] [-State <MachineCommandState>] [-User <String>] [-
ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Get the list of commands queued for delivery to a desktop. Commands are batched and can be configured to be delivered at various times during a desktop session's lifetime. Normally commands are sent within a few minutes of being queued, but it is also possible to queue a command for a user who is not currently logged on or a desktop that is currently switched off.

See about_Broker_Filtering for information about advanced filtering options.

---------- BrokerMachineCommand Object

The command object returned represents a command handled by a specific service on a desktop as determined by the Category property.

-- Category (System.String)

Category of the command.

-- CommandData (System.Byte[])

Additional binary data included when the command is sent.

-- CommandName (System.String)

Name of the command.

-- CompletionTime (System.DateTime?)

Time at which the command was sent, expired or canceled.

-- DesktopGroupNames (System.String[])

List of desktop group names that the command was restricted to.

-- MachineName (System.String)

Name of the machine this command is targeted at.

-- MachineUid (System.Int32?)

Unique ID of the machine this command is targeted at.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Metadata for this command.

-- RequestTime (System.DateTime)

Time at which this command was created.

-- SendDeadline (System.TimeSpan)

Duration after which this command expires if it has not been sent yet.

-- SendDeadlineTime (System.DateTime?)

Time at which this command expires if it has not been sent yet.

-- SendTrigger (Citrix.Broker.Admin.SDK.MachineCommandTrigger?)

Event that triggers the sending of the command. Valid values are NextContact, Broker, LogOn, Logoff, Disconnect and Reconnect.

-- SessionUid (System.Int64?)

Unique ID of the session this command is targeted at.

-- State (Citrix.Broker.Admin.SDK.MachineCommandState)

Indicates whether the command is pending, sent, expired or canceled.

-- Synchronous (System.Boolean)

Flag that indicates if this is a synchronous command.

-- Uid (System.Int64)

Unique identifier of this machine command.

-- User (System.String)

Name of the user this command is targeted at.

Related topics

New-BrokerMachineCommand

Remove-BrokerMachineCommand

Parameters

-Uid<Int64>

Get only the command with the specified unique identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Category<String>

Get only commands targeted to the specified service category.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CommandName<String>

Get only commands with the specified command name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CompletionTime<DateTime>

Get only commands that entered the Sent, Failed, Canceled or Expired state at the specified time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Get only commands targeted to the specified machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineUid<Int32>

Get only commands targeted to the specified machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-RequestTime<DateTime>

Get only commands that were requested at the specified time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SendDeadline<TimeSpan>

Get only commands that expire after the specified time span.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SendDeadlineTime<DateTime>

Get only commands that have the specified deadline time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SendTrigger<MachineCommandTrigger>

Get only commands that are due to be sent when the specified trigger occurs. Valid values are NextContact, Broker, LogOn, Logoff, Disconnect and Reconnect.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUid<Int64>

Get only commands targeted to the specified session.

Required?	false
Default Value	
Accept Pipeline Input?	false

-State<MachineCommandState>

Get only commands in the specified state. Valid values are Pending, Sent, Failed, Canceled and Expired.

Required?	false
Default Value	
Accept Pipeline Input?	false

-User<String>

Get only commands targeted to the specified user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None No parameter is accepted from the input pipeline.

Return Values

Citrix.Broker.Admin.SDK.MachineCommand

Returns Command objects matching all specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

```
Get-BrokerMachineCommand
```

Returns all pending, canceled, expired and sent commands.

---------- EXAMPLE 2 ----------

```
Get-BrokerMachineCommand -State Pending
```

Returns all queued commands.

Get-BrokerMachineConfiguration

Sep 10, 2014

Gets machine configurations defined for this site.

Syntax

```
Get-BrokerMachineConfiguration [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerMachineConfiguration [[-Name] <String>] [-ConfigurationSlotUid <Int32>] [-LeafName <String>] [-Metadata <String>] [-DesktopGroupUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Retrieves machine configurations matching the specified criteria. If no parameters are specified this cmdlet enumerates all machine configurations.

Machine configurations contain binary arrays of settings data that are managed using SDK snap-ins. Each machine configuration is associated with a configuration slot and referenced by Name. The configuration slot restricts the settings that can be held by the machine configuration. For example, only configurations for Citrix User Profile Manager can be associated with the "User Profile Manager" slot.

See about_Broker_Filtering for information about advanced filtering options.

---------- BrokerMachineConfiguration Object

The machine configuration object returned represents a named collection of related settings values that are applied to a desktop group.

-- ConfigurationSlotUid (System.Int32)

Uid of the associated configuration slot.

-- Description (System.String)

Optional description of the machine configuration.

-- DesktopGroupUids (System.Int32[])

List of desktop group Uids that this machine configuration has been added to.

-- LeafName (System.String)

Name of this machine configuration.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Map of metadata associated with this machine configuration.

-- Name (System.String)

Unique "SlotName\MachineConfigurationName" for this machine configuration.

-- Policy (System.Byte[])

A binary array of encoded settings.

-- Uid (System.Int32)

Uid of this machine configuration.

Related topics

New-BrokerMachineConfiguration

Set-BrokerMachineConfiguration

Rename-BrokerMachineConfiguration

Remove-BrokerMachineConfiguration

Add-BrokerMachineConfiguration

Parameters

-Uid<Int32>

Get only the machine configuration with the specified unique identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Get only the machine configuration with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConfigurationSlotUid<Int32>

Get only the machine configurations associated with the specified configuration slot.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LeafName<String>

Get only the machine configurations that have the specified leaf name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Get only the machine configurations that have been assigned to the specified desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error

record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.MachineConfiguration

Get-BrokerMachineConfiguration returns an object for each matching machine configuration.

Examples

---------- EXAMPLE 1 ----------

Get-BrokerMachineConfiguration
Retrieves a list of every defined machine configuration.

---------- EXAMPLE 2 ----------

Get-BrokerMachineConfiguration -Name Receiver\Engineering
Retrieves the machine configuration named "Receiver\Engineering".

---------- EXAMPLE 3 ----------

Get-BrokerMachineConfiguration -Name UPM*
Retrieves a list of every machine configuration associated with the configuration slot named "UPM".

---------- EXAMPLE 4 ----------

Get-BrokerMachineConfiguration -LeafName "Dept*"
Retrieves a list of every machine configuration with a LeafName that starts with "Dept", regardless of the associated configuration slot.

Get-BrokerMachineStartMenuShortcutIcon

Sep 10, 2014

Retrieves a Start Menu Shortcut icon from the specified machine.

Syntax

```
Get-BrokerMachineStartMenuShortcutIcon [-MachineName] <String> [-Path] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Retrieves the icon associated with a particular shortcut on a particular machine. This icon is usually used to help create a published application to access the shortcut.

Related topics

Get-BrokerMachine

New-BrokerIcon

Parameters

-MachineName<String>

Specify the name of the machine to use for icon retrieval for the specified shortcut path. The machine can be identified by DNS name, short name, SID, or name of the form domain\machine.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Path<String>

The location of the shortcut in the specified machine whose icon is being fetched.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

System.String

Get-BrokerMachineStartMenuShortcutIcon generates a Base64 encoded string containing the icon for the specified shortcut. This can be used as input to New-BrokerIcon cmdlet.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS> $shortcuts =  Get-BrokerMachineStartMenuShortcuts -MachineName 'MyDomain\MyMachine'
C:\PS> $encodedIconData =  Get-BrokerMachineStartMenuShortcutIcon -MachineName 'MyDomain\MyMachine' -Path $shortcuts[0].ShortcutPath
C:\PS> $brokerIcon = New-BrokerIcon -EncodedIconData $encodedIconData
C:\PS> Set-BrokerApplication 'Notepad' -IconUid $brokerIcon.Uid
```

This example retrieves all Start Menu Shortcuts from 'MyDomain\MyMachine', and then the icon for the first shortcut from the returned list. The icon is then associated with a published application called 'Notepad'.

Get-BrokerMachineStartMenuShortcuts

Sep 10, 2014

Retrieves the Start Menu Shortcuts from the specified machine.

Syntax

```
Get-BrokerMachineStartMenuShortcuts [-MachineName] <String> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Retrieves the shortcuts defined for all the start menu items on a particular machine. The shortcuts obtained are from the 'All users' start menu; user-specific shortcuts are not found.

Related topics

Parameters

-MachineName<String>

Specify the name of the machine to use for shortcut retrieval. The machine can be identified by DNS name, short name, SID, or name of the form domain\machine.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

None or Citrix.Broker.Admin.SDK.StartMenuShorcut

Get-BrokerMachineStartMenuShortcuts generates an array of Citrix.Broker.Admin.SDK.StartMenuShortcut objects.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $shortcuts = Get-BrokerMachineStartMenuShortcuts -MachineName 'MyDomain\MyMachine'
```

This example retrieves all Start Menu Shortcuts from 'MyDomain\MyMachine'.

Get-BrokerPowerTimeScheme

Sep 10, 2014

Gets power management time schemes for desktop groups.

Syntax

Get-BrokerPowerTimeScheme [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerPowerTimeScheme [[-Name] <String>] [-DesktopGroupUid <Int32>] [-Metadata <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Finds power time schemes matching the specified search criteria. Each desktop group in the site can have a number of power time schemes associated with it, and these time schemes control how the power states of machines in the group are managed.

If no search criteria are specified all power time schemes for all desktop groups are obtained.

Each power time scheme covers one or more days of the week, and defines which hours of those days are considered peak times and which are off-peak times. In addition, the time scheme defines a pool size value for each hour of the day for the days of the week covered by the time scheme. No one desktop group can be associated with two or more time schemes that cover the same day of the week.

For any day of the week not covered by any power time scheme, it is assumed that all hours are off-peak and no pool size management is required for any of the hours.

For more information about the power policy mechanism and pool size management, see 'help about_Broker_PowerManagement'.

---------- BrokerPowerTimeScheme Object

The BrokerPowerTimeScheme object represents a power time scheme, defining peak/off-peak hours and idle pool sizes for desktop groups. It contains the following properties:

-- DaysOfWeek (Citrix.Broker.Admin.SDK.TimeSchemeDays)

The days of the week for which this scheme applies to (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Weekdays, Weekend).

-- DesktopGroupUid (System.Int32)

The desktop group that this time scheme is for.

-- DisplayName (System.String)

The name of this time scheme, as displayed in the Studio console.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Metadata for this power time scheme.

-- Name (System.String)

The unique name of this time scheme.

-- PeakHours (System.Boolean[])

A set of 24 boolean flag values, one for each hour of the day. The first value in the array relates to midnight to 00:59, the next one to 1 AM to 01:59 and so on, with the last array element relating to 11 PM to 11:59. If the flag is $true it means that the associated hour of the day is considered a peak time; if it is $false it means that it is considered off-peak.

-- PoolSize (System.Int32[])

A set of 24 integer values, one for each hour of the day. The first value in the array relates to midnight to 00:59, the next one to 1 AM to 01:59 and so on, with the last array element relating to 11 PM to 11:59. The value defines the number of machines (either as an absolute number or a percentage of the machines in the desktop group) that are to be maintained in a running state, whether they are in use or not. A value of -1 has special meaning: pool size management does not apply during such hours.

-- PoolUsingPercentage (System.Boolean?)

A boolean flag to indicate whether the integer values in the pool size array are to be treated as absolute values (if this value is $false) or as percentages of the number of machines in the desktop group (if this value is $true).

-- Uid (System.Int32)

Unique internal identifier of a time scheme.

Related topics

New-BrokerPowerTimeScheme

Set-BrokerPowerTimeScheme

Remove-BrokerPowerTimeScheme

Rename-BrokerPowerTimeScheme

Parameters

-Uid<Int32>

Gets only the power time scheme with the specified Uid.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets only power time schemes with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets only the power time schemes associated with the specified desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False

Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	

Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.PowerTimeScheme

Get-BrokerPowerTimeScheme returns all power time schemes that match the specified selection criteria.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerPowerTimeScheme
Fetches all known power time schemes for all desktop groups in the site.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerPowerTimeScheme -DesktopGroupUid (Get-BrokerDesktopGroup 'Sales Desktops').Uid
Fetches all the power time schemes for the desktop group called 'Sales Desktops'.

Get-BrokerPrivateDesktop

Sep 10, 2014

Get private desktops configured for this site.

Syntax

Get-BrokerPrivateDesktop [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerPrivateDesktop [[-MachineName] <String>] [-AgentVersion <String>] [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-ColorDepth <ColorDepth>] [-ControllerDNSName <String>] [-Description <String>] [-DesktopGroupUid <Int32>] [-DNSName <String>] [-HostedMachineId <String>] [-HostedMachineName <String>] [-HostingServerName <String>] [-HypervisorConnectionUid <Int32>] [-IconUid <Int32>] [-InMaintenanceMode <Boolean>] [-IPAddress <String>] [-IsAssigned <Boolean>] [-LastDeregistrationReason <DeregistrationReason>] [-LastDeregistrationTime <DateTime>] [-LastHostingUpdateTime <DateTime>] [-OSType <String>] [-OSVersion <String>] [-PowerState <PowerState>] [-PublishedName <String>] [-RegistrationState <RegistrationState>] [-SecureIcaRequired <Boolean>] [-SID <String>] [-Tag <String>] [-WillShutdownAfterUse <Boolean>] [-AssignedUserSID <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

This cmdlet is deprecated, please use the Get-BrokerMachine cmdlet instead.

Retrieve private desktops matching the specified criteria. If no parameters are specified, this cmdlet enumerates all private desktops.

Get-BrokerPrivateDesktop returns configuration information only for private desktops (a DesktopKind of 'Private'). For more state information about desktops, or other types of desktop, use the Get-BrokerMachine cmdlet instead.

For information about advanced filtering options, see about_Broker_Filtering; for more information about desktops, see about_Broker_Desktops.

---------- BrokerPrivateDesktop Object

Private desktops are machines that have been configured with a DesktopKind of 'Private'. They are allocated to either a user/users or a client name/address (but cannot be allocated to both).

-- AgentVersion (System.String)

Version of the Citrix Virtual Delivery Agent (VDA) installed on the desktop.

-- AssignedClientName (System.String)

Client name the desktop has been assigned to.

-- AssignedIPAddress (System.String)

IP Address the desktop has been assigned to.

-- ColorDepth (Citrix.Broker.Admin.SDK.ColorDepth?)

The color depth setting configured on the desktop, possible values are:

$null, FourBit, EightBit, SixteenBit, and TwentyFourBit.

-- ControllerDNSName (System.String)

The DNS host name of the controller that the desktop is registered to.

-- Description (System.String)

Description of the private desktop.

-- DesktopGroupUid (System.Int32)

Uid of the desktop group the desktop has been assigned to.

-- DNSName (System.String)

The DNS host name of the desktop.

-- HostedMachineId (System.String)

Unique ID within the hosting unit of the target managed desktop.

-- HostedMachineName (System.String)

The friendly name of a hosted desktop as used by its hypervisor. This is not necessarily the DNS name of the desktop.

-- HostingServerName (System.String)

DNS name of the hypervisor that is hosting the desktop if managed.

-- HypervisorConnectionUid (System.Int32?)

The UID of the hypervisor connection that the desktop has been assigned to, if managed.

-- IconUid (System.Int32?)

The UID of the desktop's icon that is displayed in StoreFront. If this is $null then the desktop will use the icon specified by the desktop group.

-- InMaintenanceMode (System.Boolean)

Denotes whether the desktop is in maintentance mode.

-- IPAddress (System.String)

The IP address of the desktop.

-- IsAssigned (System.Boolean)

Denotes whether a private desktop has been assigned to a user/users, or a client name/address. Users can be assigned explictitly or by assigning on first use of the desktop.

-- LastDeregistrationReason (Citrix.Broker.Admin.SDK.DeregistrationReason?)

The reason for the last deregistration of the desktop with the broker. Possible values are:

AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

-- LastDeregistrationTime (System.DateTime?)

Time of the last deregistration of the desktop from the controller.

-- LastHostingUpdateTime (System.DateTime?)

Time of last update to any hosting data for this desktop reported by the hypervisor connection.

-- MachineName (System.String)

DNS host name of the machine associated with the desktop.

-- OSType (System.String)

A string that can be used to identify the operating system that is running on the desktop.

-- OSVersion (System.String)

A string that can be used to identify the version of the operating system running on the desktop, if known.

-- PowerState (Citrix.Broker.Admin.SDK.PowerState)

The current power state of the desktop. Possible values are: Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, Resuming.

-- PublishedName (System.String)

The name of the desktop that is displayed in StoreFront, if the desktop is published.

-- RegistrationState (Citrix.Broker.Admin.SDK.RegistrationState)

Indicates the registration state of the desktop. Possible values are: Unregistered, Initializing, Registered, AgentError.

-- SecureIcaRequired (System.Boolean?)

Flag indicating whether SecureICA is required or not when starting a session on the desktop.

-- SID (System.String)

Security identifier of the private desktop.

-- Uid (System.Int32)

Unique identifier of the private desktop.

-- WillShutdownAfterUse (System.Boolean)

Flag indicating whether this desktop is tainted and will be shutdown after all sessions on the desktop have ended. This flag should only ever be true on power managed, single-session desktops.

Note: The desktop will not shut down if it is in maintenance mode, but will shut down after the desktop is taken out of maintenance mode.

Related topics

Set-BrokerPrivateDesktop

Parameters

-Uid<Int32>

Gets desktops by Uid.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets desktops by machine name (in the form 'domain\machine').

Required?	false
Default Value	
Accept Pipeline Input?	false

-AgentVersion<String>

Gets desktops with a specific Citrix Virtual Delivery Agent (VDA) version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedClientName<String>

Gets desktops assigned to a specific client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedIPAddress<String>

Gets desktops assigned to a specific IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Gets desktops configured with a specific color depth.

Valid values are FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ControllerDNSName<String>

Gets desktops by the DNS name of the controller they are registered with.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets desktops by description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets desktops from a desktop group with a specific Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets desktops by DNS name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineId<String>

Gets desktops by the machine id known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets desktops by the machine name known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostingServerName<String>

Gets desktops by the name of the hosting hypervisor server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets desktops by the uid of the hosting hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Gets desktops by configured icon. Note that desktops with a $null IconUid use the icon of the desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Gets desktops by the InMaintenanceMode setting.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IPAddress<String>

Get desktops by their IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsAssigned<Boolean>

Gets desktops depending on whether they are assigned or not. Private desktops can be assigned to either a user/users or client names/addresses.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationReason<DeregistrationReason>

Gets desktops whose broker last recorded a specific deregistration reason.

Valid values are $null, AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

Required?	false
Default Value	

Accept Pipeline Input?	false

-LastDeregistrationTime<DateTime>

Gets desktops by the time that they were last deregistered.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastHostingUpdateTime<DateTime>

Gets desktops by the time that the hosting information was last updated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets desktops by the type of operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSVersion<String>

Gets desktops by the version of the operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerState<PowerState>

Gets desktops by power state.

Valid values are Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Gets desktops by published name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RegistrationState<RegistrationState>

Gets desktops by registration state.

Valid values are Registered, Unregistered, and AgentError.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Gets desktops configured with a particular SecureIcaRequired setting. Note that the desktop setting of $null indicates that the desktop group value is used.

Required?	false
Default Value	

Accept Pipeline Input?	false

-SID<String>

Gets desktops by machine SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Tag<String>

Gets desktops tagged with the given tag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WillShutdownAfterUse<Boolean>

Gets desktops depending on whether they will be automatically shut down when the current session ends or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedUserSID<String>

Gets desktops with the given assigned user (specified by SID).

Required?	false
Default Value	

Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false

Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.PrivateDesktop

Get-BrokerPrivateDesktop returns an object for each matching private desktop.

Notes

To compare dates/times, use -Filter and relative comparisons. See about_Broker_Filtering for details.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $list = 'Unmanaged','On','TurningOn','Resuming'
C:\PS> Get-BrokerPrivateDesktop -Filter { PowerState -in $list } | ft -a DNSName,PowerState
```

Get all private desktops that are turned on, or are turning on (assuming unmanaged desktops are powered on).

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerPrivateDesktop -Tag TestTag
```

Retrieve all private desktops tagged with the 'TestTag' tag.

Get-BrokerRebootCycle

Sep 10, 2014

Gets one or more reboot cycles.

Syntax

Get-BrokerRebootCycle -Uid <Int64> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerRebootCycle [-CatalogName <String>] [-CatalogUid <Int32>] [-DesktopGroupName <String>] [-DesktopGroupUid <Int32>] [-EndTime <DateTime>] [-MachinesCompleted <Int32>] [-MachinesFailed <Int32>] [-MachinesInProgress <Int32>] [-MachinesPending <Int32>] [-MachinesSkipped <Int32>] [-Metadata <String>] [-RebootDuration <Int32>] [-StartTime <DateTime>] [-State <RebootCycleState>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Get-BrokerRebootCycle cmdlet is used to enumerate reboot cycles that match all of the supplied criteria.

See about_Broker_Filtering for information about advanced filtering options.

---------- BrokerRebootCycle Object

The reboot cycle object returned represents a single occurrence of the process of rebooting a portion (or all) of the machines in a desktop group.

-- CatalogName (System.String)

Name of the catalog whose machines are rebooted by this cycle if the cycle is associated with a catalog.

-- CatalogUid (System.Int32?)

Uid of the catalog whose machines are rebooted by this cycle if the cycle is associated with a catalog.

-- DesktopGroupName (System.String)

Name of the desktop group whose machines are rebooted by this cycle.

-- DesktopGroupUid (System.Int32)

Uid of the desktop group whose machines are rebooted by this cycle.

-- EndTime (System.DateTime?)

Time at which this cycle was completed, canceled or abandoned.

-- MachinesCompleted (System.Int32)

Number of machines successfully rebooted by this cycle.

-- MachinesFailed (System.Int32)

Number of machines issued with reboot requests where either the request failed or the operation did not complete within the allowed time.

-- MachinesInProgress (System.Int32)

Number of machines issued with reboot requests but which have not yet completed the operation.

-- MachinesPending (System.Int32)

Number of outstanding machines to be rebooted during the cycle but on which processing has not yet started.

-- MachinesSkipped (System.Int32)

Number of machines scheduled for reboot during the cycle but which were not processed either because the cycle was canceled or abandoned or because the machine was unavailable for reboot processing throughout the cycle.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Map of metadata associated with this cycle.

-- RebootDuration (System.Int32)

Approximate maximum number of minutes over which the reboot cycle runs.

-- StartTime (System.DateTime)

Time of day at which this reboot cycle was started.

-- State (Citrix.Broker.Admin.SDK.RebootCycleState)

The execution state of this cycle.

-- Uid (System.Int64)

Unique ID of this reboot cycle.

-- WarningDuration (System.Int32)

Number of minutes to display the warning message for.

-- WarningMessage (System.String)

Warning message to display to users in active sessions prior to rebooting the machine.

-- WarningTitle (System.String)

Title of the warning message dialog.

Related topics

Start-BrokerRebootCycle

Stop-BrokerRebootCycle

Parameters

-Uid<Int64>

Gets reboot cycles that have the specified Uid.

Required?	true
Default Value	
Accept Pipeline Input?	false

-CatalogName<String>

Gets reboot cycles that relate to the named catalog.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogUid<Int32>

Gets reboot cycles that relate to the catalog with a particular Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets reboot cycles that relate to the named desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets reboot cycles that relate to the desktop group with a particular Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EndTime<DateTime>

Gets reboot cycles that have the specified time at which the reboot cycle was completed, canceled or abandoned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachinesCompleted<Int32>

Gets reboot cycles that have the specified count of machines successfully rebooted during the cycle.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachinesFailed<Int32>

Gets reboot cycles that have the specified count of machines issued with reboot requests where either the request failed or the operation did not complete within the allowed time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachinesInProgress<Int32>

Gets reboot cycles that have the specified count of machines issued with reboot requests but which have not yet completed the operation.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachinesPending<Int32>

Gets reboot cycles that have the specified count of outstanding machines to be rebooted during the cycle but on which processing has not yet started.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachinesSkipped<Int32>

Gets reboot cycles that have the specified count of machines scheduled for reboot during the cycle but which were not processed either because the cycle was canceled or abandoned or because the machine was unavailable for reboot processing throughout the cycle.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	

Accept Pipeline Input?	false

-RebootDuration<Int32>

Gets reboot cycles that have the specified approximate maximum duration in minutes over which the reboot cycle runs.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartTime<DateTime>

Gets reboot cycles that have the specified time at which the reboot cycle started.

Required?	false
Default Value	
Accept Pipeline Input?	false

-State<RebootCycleState>

Gets reboot cycles that have the specified overall state of the reboot cycle. Valid values are Initializing, Active, Completed, Canceled, and Abandoned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false

Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false

Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None Input cannot be piped to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.RebootCycle

Returns matching reboot cycles.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerRebootCycle
```

Enumerate all reboot cycles.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerRebootCycle -State Completed
```

Enumerates all reboot cycles that have successfully completed.

---------- EXAMPLE 3 ----------

C:\PS> Get-BrokerRebootCycle -DesktopGroupName CallCenter

Enumerates all reboot cycles related to the desktop group named CallCenter.

Get-BrokerRebootSchedule

Sep 10, 2014

Gets one or more reboot schedules.

Syntax

```
Get-BrokerRebootSchedule [-DesktopGroupUid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Get-BrokerRebootSchedule [[-DesktopGroupName] <String>] [-Active <Boolean>] [-Day <RebootScheduleDays>] [-Enabled <Boolean>] [-Frequency <RebootScheduleFrequency>] [-RebootDuration <Int32>] [-StartTime <TimeSpan>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Get-BrokerRebootSchedule cmdlet is used to enumerate desktop group reboot schedules that match all of the supplied criteria.

A reboot schedule can be configured to cause all of the machines in a desktop group to be rebooted at a particular time each day or each week, with the reboot of the individual machines spread out over the duration of the whole reboot cycle. A specific warning message can be configured to be displayed to users who are running sessions on the machines being rebooted. Note that each desktop group can only have a single reboot schedule configured.

See about_Broker_Filtering for information about advanced filtering options.

---------- BrokerRebootSchedule Object

The reboot schedule object returned represents a regularly scheduled reboot of machines in a desktop group.

-- Active (System.Boolean)

True if there is an active reboot cycle for this schedule, false otherwise.

-- Day (Citrix.Broker.Admin.SDK.RebootScheduleDays)

When the frequency is weekly, day of the week on which the schedule reboot starts.

-- DesktopGroupName (System.String)

Name of the desktop group rebooted by this schedule.

-- DesktopGroupUid (System.Int32)

Uid of the desktop group rebooted by this schedule.

-- Enabled (System.Boolean)

True if this schedule is currently enabled, false otherwise.

-- Frequency (Citrix.Broker.Admin.SDK.RebootScheduleFrequency)

Whether the schedule runs daily or weekly.

-- RebootDuration (System.Int32)

Approximate maximum number of minutes over which the scheduled reboot cycle runs.

-- StartTime (System.TimeSpan)

Time of day at which the scheduled reboot cycle starts.

-- WarningDuration (System.Int32)

Number of minutes to display the warning message for.

-- WarningMessage (System.String)

Warning message to display to users in active sessions prior to rebooting the machine.

-- WarningTitle (System.String)

Title of the warning message dialog.

Related topics

Set-BrokerRebootSchedule

New-BrokerRebootSchedule

Remove-BrokerRebootSchedule

Get-BrokerRebootCycle

Parameters

-DesktopGroupUid<Int32>

Gets the reboot schedule for the desktop group having this Uid.

Required?	true
Default Value	
Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets the reboot schedule for the desktop group having this name.

Required?	false
Default Value	

Accept Pipeline Input?	false

-Active<Boolean>

Gets desktop group reboot schedules according to whether they are currently active or not. A schedule is active if there is a reboot cycle currently running that was started as a result of the schedule.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Day<RebootScheduleDays>

Gets the reboot schedules set to run on the specified day (one of Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets the reboot schedules with the specified Enabled value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Frequency<RebootScheduleFrequency>

Gets the reboot schedules with the specified frequency (either Weekly or Daily).

Required?	false

Default Value	
Accept Pipeline Input?	false

-RebootDuration<Int32>

Gets the reboot schedules with the specified duration.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartTime<TimeSpan>

Gets the reboot schedules with the specified start time (HH:MM).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false

Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None Input cannot be piped to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.RebootSchedule

Returns matching reboot schedules.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerRebootSchedule
Enumerates all of the reboot schedules.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerRebootSchedule -Enabled $false -Frequency Daily
Enumerates all disabled reboot schedules that are scheduled to run daily.

---------- EXAMPLE 3 ----------

C:\PS> Get-BrokerRebootSchedule -DesktopGroupUid 11
Returns the unique reboot schedule for the desktop group having the Uid 11.

Get-BrokerRemotePCAccount

Sep 10, 2014

Get RemotePCAccount entries configured for this site.

Syntax

Get-BrokerRemotePCAccount -Uid <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerRemotePCAccount [-AllowSubfolderMatches <Boolean>] [-CatalogUid <Int32>] [-OU <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieves RemotePCAccounts matching the specified criteria. If no parameters are specified this cmdlet enumerates all RemotePCAccounts. Each RemotePCAccount object defines a set of machines either by machine name patterns or by where the machines are placed in Active Directory, and which RemotePC catalog the machines are to be associated with when they are discovered.

---------- BrokerRemotePCAccount Object

RemotePCAccounts define a set of machines either by machine name patterns or by where the machines are placed in Active Directory, and which RemotePC catalog the machines are to be associated with when they are discovered.

-- AllowSubfolderMatches (System.Boolean)

Specifies whether machines subfolders of specified AD OUs are to be considered part of the RemotePCAccount.

-- CatalogUid (System.Int32)

The Uid of the RemotePC catalog to which machines in the RemotePCAccount automatically join during registration.

-- MachinesExcluded (System.String[])

A list of machines which are to be excluded from the RemotePCAccount. Wildcard matching is supported.

-- MachinesIncluded (System.String[])

A list of machines which are to be included in the RemotePCAccount. Wildcard matching is supported.

-- OU (System.String)

Machines within this specified AD OU are considered part of the RemotePCAccount, unless they are in they match the MachinesExcluded

-- Uid (System.Int32)

The Uid of the RemotePCAccount object.

Related topics

New-BrokerRemotePCAccount

Set-BrokerRemotePCAccount

Remove-BrokerRemotePCAccount

Parameters

-Uid<Int32>

Gets the RemotePCAccount with the specified unique ID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AllowSubfolderMatches<Boolean>

Gets RemotePCAccounts with the specified value of AllowSubfolderMatches.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogUid<Int32>

Gets RemotePCAccounts belonging to the specified Remote PC catalog.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OU<String>

Gets the RemotePCAccount with the specified OU.

Required?	false

Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.RemotePCAccount

Get-BrokerRemotePCAccount returns an object for each matching RemotePCAccount.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerRemotePCAccount
Find all RemotePCAccounts.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerRemotePCAccount -CatalogUid 42
Find RemotePCAccounts belonging to Remote PC catalog 42.

Get-BrokerResource

Sep 10, 2014

Gets resources that a user can broker connections to.

Syntax

Get-BrokerResource [-User] <String> [-Groups <String[]>] [-ClientName <String>] [-ClientIP <String>] [-ViaAG <Boolean>] [-SmartAccessTags <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieve a list of resources that a user has access to, taking into account the site access policy, configuration of desktop groups, assignments, entitlements, and applications.

What a user has access to depends on a number of attributes:

-- User's name or security identifier.

-- Groups that the user is a member of (names or security identifiers).

-- IP address of the client the user connects from.

-- Name of the client that the user connects from.

-- Whether the user is connecting via Citrix Access Gateway.

-- SmartAccess tags when connecting via Citrix Access Gateway.

You must always specify the user's name or security identifier, but you will not always be able to predict what some of the other values will be. By omitting these values the corresponding access checks are ignored.

Consider for example, a site configuration that uses IP address ranges to allow access to private desktop A when connecting from the local network and private desktop B when connecting from home. Running this cmdlet without specifying a client IP address would return both A and B.

The output of this cmdlet depends on the available resources:

-- Assigned private desktops are returned as PrivateDesktop objects.

-- Shared desktops are returned as EntitlementPolicyRule objects.

-- Assign-On-First-Use desktops that have not been assigned yet are returned as AssignmentPolicyRule objects.

-- Application resources produce Application objects.

If more than one type of resource is available, the output pipeline contains a mixture of the above objects, in no particular order.

Only resources accessible based on the specified parameters, and visible to the administrator running this cmdlet are returned.

Related topics

Parameters

-User<String>

Gets resources given the specified user name or security identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Groups<String[]>

Get resources accessible given a list of group names or security identifiers.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientName<String>

Get resources given the specified client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientIP<String>

Get resources given the specified client IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ViaAG<Boolean>

Gets resources given the specified ViaAG setting.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SmartAccessTags<String[]>

Get resources given the specified SmartAccess tags.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.PrivateDesktop

Get-BrokerResource returns a PrivateDesktop for each accessible assigned private desktop.Citrix.Broker.Admin.SDK.EntitlementPolicyRule

Get-BrokerResource returns an EntitlementPolicyRule object for each accessible entitlement to a shared desktop.Citrix.Broker.Admin.SDK.AssignmentPolicyRule

Get-BrokerResource returns an AssignmentPolicyRule object for each accessible Assign-On-First-Use desktop.Citrix.Broker.Admin.SDK.Application

Get-BrokerResource returns an Application object for each accessible application.

Examples

---------- EXAMPLE 1 ----------

```
Get-BrokerResource -User MYDOMAIN\User1 -Group MYDOMAIN\Accounts,MYDOMAIN\Managers
```

List resources visible by User1 assuming membership of a couple of groups.

---------- EXAMPLE 2 ----------

```
[int[]]$groups = (Get-BrokerResource -User MYDOMAIN\User1 | %{ $_.DesktopGroupUid })
Get-BrokerDesktopGroup -Filter { Uid -in $groups } -Property Uid,Name
```

Get all of the desktop groups supporting the resources accessible by User1, outputting the uid and name of each desktop group.

Get-BrokerScopedObject

Sep 10, 2014

Gets the details of the scoped objects for the Broker Service.

Syntax

```
Get-BrokerScopedObject -ScopeId <Guid> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerScopedObject [-Description <String>] [-ObjectId <String>] [-ObjectName <String>] [-ObjectType <ScopedObjectType>] [-ScopeName <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a list of directly scoped objects including the names and identifiers of both the scope and object as well as the object description for display purposes.

There will be at least one result for every directly scoped object. When an object is associated with multiple scopes the output contains one result per scope duplicating the object details.

No records are returned for the All scope, though if an object is not in any scope a result with a null ScopeId and ScopeName will be returned.

---------- BrokerScopedObject Object

A scoped, or scopeable object configured in the Broker.

-- Description (System.String)

Description of the object (possibly $null if the object type does not have a description).

-- ObjectId (System.String)

Unique identifier of the object.

-- ObjectName (System.String)

Display name of the object.

-- ObjectType (Citrix.Broker.Admin.SDK.ScopedObjectType)

Type of the object this entry relates to.

-- ScopeId (System.Guid?)

Specifies the unique identifier of the scope.

-- ScopeName (System.String)

Specifies the display name of the scope.

Related topics

Parameters

-ScopeId<Guid>

Gets scoped object entries for the given scope identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets scoped object entries for objects with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ObjectId<String>

Gets scoped object entries for objects with the specified object identifier.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ObjectName<String>

Gets scoped object entries for objects with the specified object identifier.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ObjectType<ScopedObjectType>

Gets scoped object entries for objects of the given type.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScopeName<String>

Gets scoped object entries with the given scope name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Return Values

Citrix.Broker.Sdk.ScopedObject

The Get-BrokerScopedObject command returns an object containing the following properties:

ScopeId <Guid?>

Specifies the unique identifier of the scope.

ScopeName <String>

Specifies the display name of the scope.

ObjectType <ScopedObjectType>

Type of the object this entry relates to.

ObjectId <String>

Unique identifier of the object.

ObjectName <String>

Display name of the object

Description <String>

Description of the object (possibly $null if the object type does not have a description).

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-BrokerScopedObject -ObjectType Scheme

    ScopeId    : eff6f464-f1ee-4442-add3-99982e0cec01
    ScopeName  : Sales
    ObjectType : Scheme
    ObjectId   : cd4174ee-9e4b-4e57-b126-9dbf757fe493
```



```
ObjectName  : MyExampleScheme
Description : Test scheme

ScopeId     : 304e0fa7-d390-47f0-a94f-7e956a324c41
ScopeName   : Finance
ObjectType  : Scheme
ObjectId    : cd4174ee-9e4b-4e57-b126-9dbf757fe493
ObjectName  : MyExampleScheme
Description : Test scheme

ScopeId     :
ScopeName   :
ObjectType  : Scheme
ObjectId    : 5062e46b-71bc-4ac9-901a-30fe6797e2f6
ObjectName  : AnotherScheme
Description : Another scheme in no scopes
```

Gets all of the scoped objects with type Scheme. The example output shows a scheme object (MyExampleScheme) in two scopes Sales and Finance, and another scheme (AnotherScheme) that is not in any scope. The ScopeId and ScopeName values returned are null in the final record.

Get-BrokerServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the Broker Service on the controller.

Syntax

```
Get-BrokerServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the Broker Service on the controller to be detected.

There is no requirement for a database connection to be configured in order for this command to be used.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

System.String

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-BrokerServiceAddedCapability
```

Get the added capabilities of the Broker Service.

Get-BrokerServiceInstance

Sep 10, 2014

Gets the service instance entries for the Broker Service.

Syntax

```
Get-BrokerServiceInstance [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns service interfaces published by instances of the Broker Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Get-BrokerServiceStatus

Reset-BrokerServiceGroupMembership

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Return Values

Citrix.Broker.Sdk.ServiceInstance

The Get-BrokerServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

Specifies the service instance type. For this service, the service instance type is always Broker.

Address

Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

SDK - for PowerShell operations

InterService - for operations between different services

Peer - for communications between services of the same type

Metadata <Citrix.Broker.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-BrokerServiceInstance
```

Get all instances of the Broker Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-BrokerServiceStatus

Sep 10, 2014

Gets the current state of the Broker Service on the controller.

Syntax

```
Get-BrokerServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the Broker Service on the controller to be determined. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured. Before using this command, you don't have to configure the database connection to the Service.

Related topics

Set-BrokerDBConnection

Test-BrokerDBConnection

Get-BrokerDBConnection

Get-BrokerDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-BrokerServiceStatus command returns an object containing the status of the Broker Service together with extra diagnostics information.

DBUnconfigured

The Broker Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the Broker Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Broker Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBMissingOptionalFeature

The Broker is connected to a database that is valid, but it does not have the full functionality required for optimal performance. Upgrading the database is advisable.

DBMissingMandatoryFeature

The Broker is connected to a database that is valid, but it does not have the full functionality required so the Broker cannot function. Upgrading the database is required.

DBNewerVersionThanService

The version of the Broker Service currently in use is incompatible with the version of the Broker Service schema on the database. Upgrade the Broker Service to a more recent version.

DBOlderVersionThanService

The version of the Broker Service schema on the database is incompatible with the version of the Broker Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Broker Service is running and is connected to a database containing a valid schema.

PendingFailure

Connectivity between the Broker Service and the database has been lost. This may be a transitory network error, but may indicate a loss of connectivity that requires administrator intervention.

Failed

Connectivity between the Broker and the database has been lost for an extended period of time, or has failed due to a configuration problem. The Broker service cannot operate while its connection to the database is unavailable.

Unknown

The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-BrokerServiceStatus
```

Get the current status of the Broker Service.

Get-BrokerSession

Sep 10, 2014

Gets a list of sessions.

Syntax

Get-BrokerSession [-Uid] <Int64> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerSession [[-SessionKey] <Guid>] [-AgentVersion <String>] [-ApplicationInUse <String>] [-AppState <SessionAppState>] [-AppStateLastChangeTime <DateTime>] [-AutonomouslyBrokered <Boolean>] [-BrokeringDuration <Int32>] [-BrokeringTime <DateTime>] [-BrokeringUserName <String>] [-BrokeringUserSID <String>] [-CatalogName <String>] [-ClientAddress <String>] [-ClientName <String>] [-ClientPlatform <String>] [-ClientProductId <Int32>] [-ClientVersion <String>] [-ConnectedViaHostName <String>] [-ConnectedViaIP <String>] [-ConnectionMode <ConnectionMode>] [-ControllerDNSName <String>] [-DesktopGroupName <String>] [-DesktopGroupUid <Int32>] [-DesktopKind <DesktopKind>] [-DesktopSID <String>] [-DesktopUid <Int32>] [-DeviceId <String>] [-DNSName <String>] [-EstablishmentDuration <Int32>] [-EstablishmentTime <DateTime>] [-HardwareId <String>] [-Hidden <Boolean>] [-HostedMachineName <String>] [-HostingServerName <String>] [-HypervisorConnectionName <String>] [-ImageOutOfDate <Boolean>] [-InMaintenanceMode <Boolean>] [-IPAddress <String>] [-IsAnonymousUser <Boolean>] [-IsPhysical <Boolean>] [-LaunchedViaHostName <String>] [-LaunchedViaIP <String>] [-LogoffInProgress <Boolean>] [-LogonInProgress <Boolean>] [-MachineName <String>] [-MachineSummaryState <DesktopSummaryState>] [-MachineUid <Int32>] [-Metadata <String>] [-OSType <String>] [-PersistUserChanges <PersistUserChanges>] [-PowerState <PowerState>] [-Protocol <String>] [-ProvisioningType <ProvisioningType>] [-ReceiverIPAddress <String>] [-ReceiverName <String>] [-SecureIcaActive <Boolean>] [-SessionId <Int32>] [-SessionState <SessionState>] [-SessionStateChangeTime <DateTime>] [-SessionSupport <SessionSupport>] [-SessionType <SessionType>] [-StartTime <DateTime>] [-UntrustedUserName <String>] [-UserFullName <String>] [-UserName <String>] [-UserSID <String>] [-UserUPN <String>] [-ApplicationUid <Int32>] [-SharedDesktopUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieves sessions matching all the specified criteria. If no parameters are specified this cmdlet enumerates all sessions.

---------- BrokerSession Object

The session object returned represents a session on a machine in the site. The session could be for a desktop or application

-- AgentVersion (System.String)

Version of the Citrix Virtual Delivery Agent (VDA) installed on the machine.

-- ApplicationsInUse (System.String[])

List of applications in use in the session. Applications are identified by their administrative name.

-- AppState (Citrix.Broker.Admin.SDK.SessionAppState)

The app state of the session. Valid values are PreLogon, PreLaunched, Active, Desktop, Lingering and NoApps.

-- AppStateLastChangeTime (System.DateTime?)

The time when the session entered the current app state.

-- AutonomouslyBrokered (System.Boolean)

Indicates whether this is an HDX session established by direct connection without being brokered.

-- BrokeringDuration (System.Int32?)

Time taken to broker the session (in milliseconds).

-- BrokeringTime (System.DateTime?)

Time at which the session was brokered.

-- BrokeringUserName (System.String)

The user name of the brokering user.

-- BrokeringUserSID (System.String)

The SID of the brokering user.

-- CatalogName (System.String)

The name of the catalog that the machine hosting the session is assigned to.

-- ClientAddress (System.String)

The IP address of the client connected to the session.

-- ClientName (System.String)

The host name of the client connected to the session.

-- ClientPlatform (System.String)

The name of client platform, as indicated by client product ID.

-- ClientProductId (System.Int32?)

The product ID of the client connected to the session.

-- ClientVersion (System.String)

The version of the Citrix Receiver running on the client connected to the session.

-- ConnectedViaHostName (System.String)

The host name of the incoming connection. This is usually a gateway, router or client.

-- ConnectedViaIP (System.String)

The IP address of the incoming connection This is usually a gateway, router or client.

-- ConnectionMode (Citrix.Broker.Admin.SDK.ConnectionMode?)

The way in which the most recent connection to the session was established. Valid modes are:

o Brokered: established through the XenDesktop Broker (for example, using StoreFront).

o Unbrokered: direct connection (for example, using the console or direct RDP/HDX).

o LeasedConnection: established through the XenDesktop Broker using a connection lease.

o VdaHighAvailabilityMode: direct connection while VDA in high-availability mode.

o ThirdPartyBroker: established through a third-party Broker.

o ThirdPartyBrokerWithLicensing: established and licensed through a third-party Broker.

-- ControllerDNSName (System.String)

The DNS host name of the controller that the session's hosting machine is registered with.

-- DesktopGroupName (System.String)

Name of the desktop group of the machine the session is on.

-- DesktopGroupUid (System.Int32)

UID of the desktop group of the machine the session is on.

-- DesktopKind (Citrix.Broker.Admin.SDK.DesktopKind)

Indicates if the session is shared or private.

-- DesktopSID (System.String)

The Windows SID of the machine the session is on.

-- DesktopUid (System.Int32)

For a desktop session, the unique identifier of the desktop.

-- DeviceId (System.String)

Unique identifier for the client device that has most recently been associated with the session.

-- DNSName (System.String)

The DNS host name of the machine hosting the session.

-- EstablishmentDuration (System.Int32?)

Duration that it took to establish the session.

-- EstablishmentTime (System.DateTime?)

Time at which the session was established.

-- HardwareId (System.String)

Unique identifier for the client hardware that has been most recently associated with the session.

-- Hidden (System.Boolean)

Flag to indicate if the session is currently hidden from the user and not to be reconnected to.

-- HostedMachineName (System.String)

The friendly name of a hosted machine running the session, as used by its hypervisor. This does not necessarily match either the DNS or AD name of the machine.

-- HostingServerName (System.String)

DNS name of the hypervisor that is hosting the machine hosting the session.

-- HypervisorConnectionName (System.String)

The name of the hypervisor connection that the machine hosting the session has been assigned to.

-- ImageOutOfDate (System.Boolean?)

Denotes whether the VM image for a hosted machine is out of date and due to be updated to a new master image when the machine next reboots.

-- InMaintenanceMode (System.Boolean)

Denotes whether the machine hosting the session is in maintentance mode.

-- IPAddress (System.String)

The IP address of the machine hosting the session.

-- IsAnonymousUser (System.Boolean)

Indicates whether the session was established anonymously (without user credentials), in this case a temporary local user account on the machine is used.

-- IsPhysical (System.Boolean)

This value is false if the machine hosting the session can be power managed, and true otherwise

-- LaunchedViaHostName (System.String)

The host name of the StoreFront server used to launch the session.

-- LaunchedViaIP (System.String)

The IP address of the StoreFront server used to launch the session.

-- LogoffInProgress (System.Boolean)

Indicates whether the session is in the process of being logged off.

-- LogonInProgress (System.Boolean)

Indicates whether the session is still executing user logon processing or not.

-- MachineName (System.String)

DNS host name of the machine hosting the session.

-- MachineSummaryState (Citrix.Broker.Admin.SDK.DesktopSummaryState)

The summary state of the machine (will be Unregistered, Disconnected, or InUse)

-- MachineUid (System.Int32)

UID of the machine hosting the session.

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

Map of metadata for this session.

-- OSType (System.String)

A string that can be used to identify the operating system that is running on the machine hosting the session.

-- PersistUserChanges (Citrix.Broker.Admin.SDK.PersistUserChanges)

Describes whether/how the user changes are persisted. Possible values are:

o OnLocal - Persist the user changes locally.

o Discard - Discard user changes.

o OnPvd - Persist user changes on the Citrix Personal vDisk.

-- PowerState (Citrix.Broker.Admin.SDK.PowerState)

The current power state of the machine hosting the session. Possible values are: Unmanaged, Unknown, Unavailable, On, Suspended, TurningOn, TurningOff, Suspending and Resuming.

-- Protocol (System.String)

The protocol that the session is using, can be HDX, RDP, or Console. Console sessions on XenDesktop 5 VDAs appear with a blank protocol.

-- ProvisioningType (Citrix.Broker.Admin.SDK.ProvisioningType)

Describes how the machine hosting the session was provisioned, possible values are:

o Manual: No provisioning.

o PVS: Machine provisioned by PVS (may be physical, blade, VM,...)

o MCS: Machine provisioned by MCS (machine must be VM)

-- ReceiverIPAddress (System.String)

The IP address of the client as supplied by Receiver (for example, StoreFront) when the session was launched, or reconnected.

-- ReceiverName (System.String)

The name of the client as supplied by Receiver (for example, StoreFront) when the session was launched, or reconnected.

-- SecureIcaActive (System.Boolean?)

Indicates whether SecureICA is active on the session.

-- SessionId (System.Int32)

Deprecated. A unique identifier that Remote Desktop Services uses to track the session but it is only unique on that machine.

-- SessionKey (System.Guid)

GUID that provides a unique identifier for this session.

-- SessionState (Citrix.Broker.Admin.SDK.SessionState)

The state of the session. Valid values are Connected, Active or Disconnected.

For a session on a machine with functional level below L7, the additional states PreparingSession, Reconnecting, NonBrokeredSession, Other, and Unknown can also occur.

-- SessionStateChangeTime (System.DateTime)

The time of the most recent state change for the session.

-- SessionSupport (Citrix.Broker.Admin.SDK.SessionSupport)

Indicates if the machine hosting the session supports multiple or single sessions.

-- SessionType (Citrix.Broker.Admin.SDK.SessionType)

Indicates if this is an Application or Desktop session.

-- SmartAccessTags (System.String[])

The Smart Access tags for this session.

-- StartTime (System.DateTime?)

Indicates when the session was started.

-- Uid (System.Int64)

Unique identifier of this session.

-- UntrustedUserName (System.String)

The name of the logged-on user reported directly from the machine (in the form DOMAIN\user). This may be useful where

the user is logged in to a non-domain account, however the name cannot be verified and must therefore be considered untrusted.

-- UserFullName (System.String)

The full name of the user.

-- UserName (System.String)

The name of the user.

-- UserSID (System.String)

The user's Windows SID.

-- UserUPN (System.String)

The user's User Principal Name

Related topics

Disconnect-BrokerSession

Stop-BrokerSession

Get-BrokerDesktop

Parameters

-Uid<Int64>

Get session by its Uid.

Required?	true
Default Value	
Accept Pipeline Input?	false

-SessionKey<Guid>

Gets session having the specified unique key.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AgentVersion<String>

Gets sessions with a specific Virtual Desktop Agent version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationInUse<String>

Gets sessions running specific applications (identified by their SDK Name property).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AppState<SessionAppState>

Get sessions by their app state.

Valid values are PreLogon, PreLaunched, Active, Desktop, Lingering and NoApps.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AppStateLastChangeTime<DateTime>

Get sessions by their app state change time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AutonomouslyBrokered<Boolean>

Gets sessions according to whether they are autonomously brokered or not. Autonomously brokered sessions are HDX sessions established by direct connection without being brokered.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringDuration<Int32>

Gets session with a specific time taken to broker. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringTime<DateTime>

Get sessions brokered at a specific time. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringUserName<String>

Get sessions by brokering user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringUserSID<String>

Get sessions by brokering user SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogName<String>

Gets sessions on machines from a specific catalog name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientAddress<String>

Get sessions by client IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientName<String>

Get sessions by client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientPlatform<String>

Get sessions by client platform.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientProductId<Int32>

Get sessions by client product ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientVersion<String>

Get sessions by client version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectedViaHostName<String>

Get sessions by host name of the incoming connection. This is usually a proxy or Citrix Access Gateway server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectedViaIP<String>

Get sessions by IP address of the incoming connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectionMode<ConnectionMode>

Gets sessions by the way in which the most recent connection to the session was established.

Valid modes are Brokered, Unbrokered, LeasedConnection, VdaHighAvailabilityMode, ThirdPartyBroker, and ThirdPartyBrokerWithLicensing.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ControllerDNSName<String>

Gets sessions that are hosted on machines which are registered with a specific controller.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets sessions from a desktop group with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets sessions from a desktop group with the specified UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopKind<DesktopKind>

Gets sessions on a desktop of a particular kind.

Valid values are Private and Shared.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopSID<String>

Get sessions by desktop SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopUid<Int32>

Get sessions by desktop Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeviceId<String>

Get sessions by client device id.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets sessions by their machine's DNS name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EstablishmentDuration<Int32>

Gets sessions which took a specific time to establish. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EstablishmentTime<DateTime>

Gets sessions which became established at a particular time. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HardwareId<String>

Get sessions by client hardware id.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Hidden<Boolean>

Get sessions by whether they are hidden or not. Hidden sessions are treated as though they do not exist when brokering sessions; a hidden session cannot be reconnected to, but a new session may be launched using the same entitlement.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets sessions by their machine's name as known to its hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostingServerName<String>

Gets sessions hosted by a machine with a specific name of the hosting hypervisor server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionName<String>

Gets sessions hosted by a machine with a specific name of the hosting hypervisor connection.

Required?	false

Default Value	
Accept Pipeline Input?	false

-ImageOutOfDate<Boolean>

Gets sessions hosted by a machine with a specific ImageOutOfDate setting.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Gets sessions hosted by a machine with a specific InMaintenanceMode setting.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IPAddress<String>

Gets sessions hosted by a machine with a specific IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsAnonymousUser<Boolean>

Gets sessions depending on whether they were established anonymously ($true) or not ($false). An anonymous session is established without user credentials and a temporary local user account is used.

Required?	false

Default Value	
Accept Pipeline Input?	false

-IsPhysical<Boolean>

Gets sessions hosted on machines where the flag indicating if the machine can be power managed by the Citrix Broker Service matches the requested value. Where the power state of the machine cannot be controlled, specify $true, otherwise $false.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LaunchedViaHostName<String>

Get sessions by the host name of the Web Interface server from which a user launches a session.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LaunchedViaIP<String>

Get sessions by the IP address of the Web Interface server from which a user launches a session.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LogoffInProgress<Boolean>

Gets sessions by whether they are in the process of being logged off or not.

Required?	false

Default Value	
Accept Pipeline Input?	false

-LogonInProgress<Boolean>

Gets sessions by whether they are still executing user logon processing or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets sessions by their machine name (in the form DOMAIN\machine).

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineSummaryState<DesktopSummaryState>

Gets sessions on a machine with a specific summary state.

Valid values are Off, Unregistered, Available, Disconnected, Preparing, and InUse.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineUid<Int32>

Gets sessions on a machine with the specified UID.

Required?	false

Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets sessions with a specific type of operating system.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PersistUserChanges<PersistUserChanges>

Gets sessions where the user changes are persisted in a particular manner. Values can be:

o OnLocal - User changes are persisted locally.

o Discard - User changes are discarded.

o OnPvd - User changes are persisted on the Pvd.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerState<PowerState>

Gets sessions on machines in the specified power state.

Valid values are Unmanaged, Unknown, Unavailable, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Protocol<String>

Get sessions by connection protocol. Valid values are HDX, RDP, or Console.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningType<ProvisioningType>

Gets sessions hosted on machines provisioned in a particular manner. Values can be:

o Manual - No automated provisioning.

o PVS - Machine provisioned by PVS (machine may be physical, blade, VM,...).

o MCS - Machine provisioned by MCS (machine must be VM).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReceiverIPAddress<String>

Gets sessions with the specified client IP address supplied by Receiver (for example, StoreFront) when the session was launched, or reconnected.

Required?	false

Default Value	
Accept Pipeline Input?	false

-ReceiverName<String>

Gets sessions with the specified client name supplied by Receiver (for example, StoreFront) when the session was launched, or reconnected.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaActive<Boolean>

Get sessions by their use of SecureICA.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionId<Int32>

Deprecated.

Gets sessions by session ID, a unique identifier that Remote Desktop Services uses to track the session but it is only unique on that machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionState<SessionState>

Get sessions by their state.

Valid values are Other, PreparingNewSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession, and Unknown.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionStateChangeTime<DateTime>

Get sessions by their last state change time. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSupport<SessionSupport>

Gets sessions hosted on machines which support the required pattern of sessions. Values can be:

o SingleSession - Single-session only machine.

o MultiSession - Multi-session capable machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionType<SessionType>

Get sessions by their type.

Valid values are Application and Desktop.

Required?	false
Default Value	

Accept Pipeline Input?	false

-StartTime<DateTime>

Get sessions by their start time. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UntrustedUserName<String>

Gets sessions by the untrusted user name reported directly from the machine (in the form DOMAIN\user).

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserFullName<String>

Gets sessions by user's full name (usually 'first-name last-name').

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserName<String>

Get sessions by user name (in the form DOMAIN\user).

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserSID<String>

Get sessions by user's Windows SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserUPN<String>

Gets sessions by user's User Principal Name (in the form user@domain).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationUid<Int32>

Get sessions running the application with the specified Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SharedDesktopUid<Int32>

Get sessions by SharedDesktop Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Session

Returns sessions matching the specified criteria.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerSession

Enumerate all sessions.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerSession -UserName MyDomain\MyAccount -SessionState Disconnected

Get all disconnected sessions for a specific user.

Get-BrokerSessionLinger

Sep 10, 2014

Gets one or more session lingering settings.

Syntax

```
Get-BrokerSessionLinger [-DesktopGroupUid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerSessionLinger [[-DesktopGroupName] <String>] [-AssociatedUserFullName <String>] [-AssociatedUserName <String>] [-AssociatedUserUPN <String>] [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-UserSID <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Get-BrokerSessionLinger cmdlet is used to enumerate desktop group session linger settings that match all of the supplied criteria.

Without parameters, Get-BrokerSessionLinger gets all the session linger settings that have been created. You can also use the parameters of Get-BrokerSessionLinger to filter the results to just the desktop group you're interested in.

Note that each desktop group can only have a single session linger setting. Session lingering only applies to application sessions.

See about_Broker_Filtering for information about advanced filtering options.

---------- BrokerSessionLinger Object

The session linger object returned represents a session linger setting in a desktop group.

-- AssociatedUserFullNames (System.String[])

List of associated users (full names). Associated users is the list of users who are given access using the pre-launch/user mapping filter.

-- AssociatedUserNames (System.String[])

List of associated users (SAM names). Associated users is the list of users who are given access using the pre-launch/user mapping filter.

-- AssociatedUserUPNs (System.String[])

List of associated users (user principle names). Associated users is the list of users who are given access using the pre-launch/user mapping filter.

-- DesktopGroupName (System.String)

Name of the associated desktop group.

-- DesktopGroupUid (System.Int32)

Uid of the associated desktop group.

-- Enabled (System.Boolean)

Specifies whether or not session lingering is enabled for the desktop group.

-- MaxAverageLoadThreshold (System.Int32)

Specifies the average load threshold across the desktop group. After this threshold is hit lingering sessions will be terminated to reduce average load across the group. Sessions that have been lingering the longest will be chosen first.

-- MaxLoadPerMachineThreshold (System.Int32)

Specifies the maximum load threshold per machine in the desktop group. After this threshold is hit lingering sessions on loaded machines will be terminated to reduce load. Sessions that have been lingering the longest will be chosen first.

-- MaxTimeBeforeDisconnect (System.TimeSpan)

Specifies the maximum time by when a lingering session will be disconnected. The disconnect timer cannot be greater than the terminate timer. When the disconnect timer is same as the terminate timer, the session will be directly be terminated. The default value is 15 minutes. A value of 0 disables the disconnect timer.

-- MaxTimeBeforeTerminate (System.TimeSpan)

Specifies the maximum time by when a lingering session will be terminated. When the disconnect timer is same as the terminate timer, the session will be directly be terminated. The default value is 8 hours. A value of 0 disables the terminate timer.

-- UserFilterEnabled (System.Boolean)

Indicates if linger-specific user filter is enabled.

Related topics

New-BrokerSessionLinger

Set-BrokerSessionLinger

Remove-BrokerSessionLinger

Parameters

-DesktopGroupUid<Int32>

Gets session linger setting that is associated with the specified desktop group Uid.

Required?	true
Default Value	

Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets session linger setting that is associated with the specified desktop group name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserFullName<String>

Gets session linger settings with an associated user identified by their full name (usually 'first-name last-name'). If the 'UserFilterEnabled' property is true then access to the session linger is restricted to those users only, otherwise access is unrestricted (but always subject to other policy rules).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserName<String>

Gets session linger settings with an associated user identified by their user name (in the form 'domain\user'). If the 'UserFilterEnabled' property is true then access to the session linger is restricted to those users only, otherwise access is unrestricted (but always subject to other policy rules).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserUPN<String>

Gets session linger settings with an associated user identified by their user principle name (in the form 'user@domain'). If the 'UserFilterEnabled' property is true then access to the session linger is restricted to those users only, otherwise access is unrestricted (but always subject to other policy rules).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets only the session linger settings that have the specified value for whether the setting is enabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxAverageLoadThreshold<Int32>

Gets only the session linger settings that have the specified average load threshold.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxLoadPerMachineThreshold<Int32>

Gets only the session linger settings that have the specified maximum load threshold per machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxTimeBeforeDisconnect<TimeSpan>

Gets only the session linger settings that have the specified idle disconnect time.

Required?	false

Default Value	
Accept Pipeline Input?	false

-MaxTimeBeforeTerminate<TimeSpan>

Gets only the session linger settings that have the specified idle terminate time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserFilterEnabled<Boolean>

Gets only session linger settings whose user filter is in the specified state.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserSID<String>

Gets only session linger settings with their accessibility restricted to include the specified user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false

Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.SessionLinger

Get-BrokerSessionLinger returns an object for each session linger setting it gets.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerSessionLinger -DesktopGroupName "test"
```

Returns the session linger settings associated with the destkop group named 'test'.

Get-BrokerSessionPreLaunch

Sep 10, 2014

Gets one or more session pre-launch settings.

Syntax

```
Get-BrokerSessionPreLaunch [-DesktopGroupUid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerSessionPreLaunch [[-DesktopGroupName] <String>] [-AssociatedUserFullName <String>] [-AssociatedUserName <String>] [-AssociatedUserUPN <String>] [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-UserSID <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Get-BrokerSessionPreLaunch cmdlet is used to enumerate desktop group session pre-launch settings that match all of the supplied criteria.

Without parameters, Get-BrokerSessionPreLaunch gets all the session pre-launch settings that have been created. You can also use the parameters of Get-BrokerSessionPreLaunch to filter the results to just the desktop group you're interested in.

Note that each desktop group can only have a single session pre-launch setting. Session pre-launch only applies to application sessions.

See about_Broker_Filtering for information about advanced filtering options.

---------- BrokerSessionPreLaunch Object

The session pre-launch object returned represents a session pre-launch setting in a desktop group.

-- AssociatedUserFullNames (System.String[])

List of associated users (full names). Associated users is the list of users who are given access using the pre-launch/user mapping filter.

-- AssociatedUserNames (System.String[])

List of associated users (SAM names). Associated users is the list of users who are given access using the pre-launch/user mapping filter.

-- AssociatedUserUPNs (System.String[])

List of associated users (user principle names). Associated users is the list of users who are given access using the pre-launch/user mapping filter.

-- DesktopGroupName (System.String)

Name of the associated desktop group.

-- DesktopGroupUid (System.Int32)

Uid of the associated desktop group.

-- Enabled (System.Boolean)

Specifies whether or not session pre-launch is enabled for the desktop group.

-- MaxAverageLoadThreshold (System.Int32)

Specifies the average load threshold across the desktop group. After this threshold is hit pre-launched sessions will be terminated to reduce average load across the group. Sessions that have been pre-launched the longest will be chosen first.

-- MaxLoadPerMachineThreshold (System.Int32)

Specifies the maximum load threshold per machine in the desktop group. After this threshold is hit pre-launched sessions on loaded machines will be terminated to reduce load. Sessions that have been pre-launched the longest will be chosen first.

-- MaxTimeBeforeDisconnect (System.TimeSpan)

Specifies the maximum time by when a pre-launched session will be disconnected. The disconnect timer cannot be greater than the terminate timer. When the disconnect timer is same as the terminate timer, the session will be directly be terminated. The default value is 15 minutes. A value of 0 disables the disconnect timer.

-- MaxTimeBeforeTerminate (System.TimeSpan)

Specifies the maximum time by when a pre-launched session will be terminated. When the disconnect timer is same as the terminate timer, the session will be directly be terminated. The default value is 8 hours. A value of 0 disables the terminate timer.

-- UserFilterEnabled (System.Boolean)

Indicates if pre-launch-specific user filter is enabled.

Related topics

New-BrokerSessionPreLaunch

Set-BrokerSessionPreLaunch

Remove-BrokerSessionPreLaunch

Parameters

-DesktopGroupUid<Int32>

Gets session pre-launch setting that is associated with the specified desktop group Uid.

Required?	true
Default Value	

Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets session pre-launch setting that is associated with the specified desktop group name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserFullName<String>

Gets session pre-launch settings with an associated user identified by their full name (usually 'first-name last-name'). If the 'UserFilterEnabled' property is true then access to the session pre-launch is restricted to those users only, otherwise access is unrestricted (but always subject to other policy rules).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserName<String>

Gets session pre-launch settings with an associated user identified by their user name (in the form 'domain\user'). If the 'UserFilterEnabled' property is true then access to the session pre-launch is restricted to those users only, otherwise access is unrestricted (but always subject to other policy rules).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserUPN<String>

Gets session pre-launch settings with an associated user identified by their user principle name (in the form 'user@domain'). If the 'UserFilterEnabled' property is true then access to the session pre-launch is restricted to those users only, otherwise access is unrestricted (but always subject to other policy rules).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Gets only the session pre-launch settings that have the specified value for whether the setting is enabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxAverageLoadThreshold<Int32>

Gets only the session pre-launch settings that have the specified average load threshold.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxLoadPerMachineThreshold<Int32>

Gets only the session pre-launch settings that have the specified maximum load threshold per machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxTimeBeforeDisconnect<TimeSpan>

Gets only the session pre-launch settings that have the specified idle disconnect time.

Required?	false

Default Value	
Accept Pipeline Input?	false

-MaxTimeBeforeTerminate<TimeSpan>

Gets only the session pre-launch settings that have the specified idle terminate time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserFilterEnabled<Boolean>

Gets only session pre-launch settings whose user filter is in the specified state.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserSID<String>

Gets only session pre-launch settings with their accessibility restricted to include the specified user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false

Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.SessionPreLaunch

Get-BrokerSessionPreLaunch returns an object for each session pre-launch setting it gets.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerSessionPreLaunch -DesktopGroupName "test"
```

Returns the session pre-launch settings associated with the destkop group named 'test'.

Get-BrokerSharedDesktop

Sep 10, 2014

Get shared desktops configured for this site.

Syntax

Get-BrokerSharedDesktop [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerSharedDesktop [[-MachineName] <String>] [-AgentVersion <String>] [-ControllerDNSName <String>] [-DesktopGroupUid <Int32>] [-DNSName <String>] [-HostedMachineId <String>] [-HostedMachineName <String>] [-HostingServerName <String>] [-HypervisorConnectionUid <Int32>] [-InMaintenanceMode <Boolean>] [-IPAddress <String>] [-LastDeregistrationReason <DeregistrationReason>] [-LastDeregistrationTime <DateTime>] [-LastHostingUpdateTime <DateTime>] [-OSType <String>] [-OSVersion <String>] [-PowerState <PowerState>] [-RegistrationState <RegistrationState>] [-SID <String>] [-Tag <String>] [-WillShutdownAfterUse <Boolean>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

This cmdlet is deprecated, please use the Get-BrokerMachine cmdlet instead.

Retrieve shared desktops matching the specified criteria. If no parameters are specified, all shared desktops are enumerated.

Get-BrokerSharedDesktop returns configuration information only for shared desktops (a DesktopKind of 'Shared').

For information about advanced filtering options, see about_Broker_Filtering; for information about desktops, see about_Broker_Desktops.

---------- BrokerSharedDesktop Object

Shared desktops are desktops that are assigned randomly to users upon connection from a pool of available machines.

-- AgentVersion (System.String)

Version of the Citrix Virtual Delivery Agent (VDA) installed on the desktop.

-- ControllerDNSName (System.String)

The DNS host name of the controller that the desktop is registered to.

-- DesktopGroupUid (System.Int32)

Uid of the desktop group the desktop has been assigned to.

-- DNSName (System.String)

The DNS host name of the desktop.

-- HostedMachineId (System.String)

Unique ID within the hosting unit of the target managed desktop.

-- HostedMachineName (System.String)

The friendly name of a hosted desktop as used by its hypervisor. This is not necessarily the DNS name of the desktop.

-- HostingServerName (System.String)

DNS name of the hypervisor that is hosting the desktop if managed.

-- HypervisorConnectionUid (System.Int32?)

The UID of the hypervisor connection that the desktop has been assigned to, if managed.

-- InMaintenanceMode (System.Boolean)

Denotes whether the desktop is in maintentance mode.

-- IPAddress (System.String)

The IP address of the desktop.

-- LastDeregistrationReason (Citrix.Broker.Admin.SDK.DeregistrationReason?)

The reason for the last deregistration of the desktop with the broker. Possible values are:

AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

-- LastDeregistrationTime (System.DateTime?)

Time of the last deregistration of the desktop from the controller.

-- LastHostingUpdateTime (System.DateTime?)

Time of last update to any hosting data for this desktop reported by the hypervisor connection.

-- MachineName (System.String)

DNS host name of the machine associated with the desktop.

-- OSType (System.String)

A string that can be used to identify the operating system that is running on the desktop.

-- OSVersion (System.String)

A string that can be used to identify the version of the operating system running on the desktop, if known.

-- PowerState (Citrix.Broker.Admin.SDK.PowerState)

The current power state of the desktop. Possible values are: Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, resuming.

-- RegistrationState (Citrix.Broker.Admin.SDK.RegistrationState)

Indicates the registration state of the desktop. Possible values are: Unregistered, Initializing, Registered, AgentError.

-- SID (System.String)

The security identifier of the shared desktop.

-- Uid (System.Int32)

The uid of the shared desktop.

-- WillShutdownAfterUse (System.Boolean)

Flag indicating whether this desktop is tainted and will be shutdown after all sessions on the desktop have ended. This flag should only ever be true on power managed, single-session desktops.

Note: The desktop will not shut down if it is in maintenance mode, but will shut down after the desktop is taken out of maintenance mode.

Related topics

Set-BrokerSharedDesktop

Parameters

-Uid<Int32>

Gets desktops by Uid.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets desktops by machine name (in the form 'domain\machine').

Required?	false
Default Value	
Accept Pipeline Input?	false

-AgentVersion<String>

Gets desktops with a specific Virtual Desktop Agent version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ControllerDNSName<String>

Gets desktops by the DNS name of the controller they are registered with.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets desktops from a desktop group with a specific Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets desktops by DNS name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineId<String>

Gets desktops by the machine id known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets desktops by the machine name known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostingServerName<String>

Gets desktops by the name of the hosting hypervisor server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets desktops by the uid of the hosting hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Gets desktops by the InMaintenanceMode setting.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IPAddress<String>

Gets desktops by IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationReason<DeregistrationReason>

Gets desktops whose broker last recorded a specific deregistration reason.

Valid values are $null, AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationTime<DateTime>

Gets desktops by the time that they were last deregistered.

Required?	false
Default Value	

Accept Pipeline Input?	false

-LastHostingUpdateTime<DateTime>

Gets desktops by the time that the hosting information was last updated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets desktops by the type of operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSVersion<String>

Gets desktops by the version of the operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerState<PowerState>

Gets desktops by power state.

Valid values are Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.

Required?	false
Default Value	

Accept Pipeline Input?	false

-RegistrationState<RegistrationState>

Gets desktops by registration state.

Valid values are Registered, Unregistered, and AgentError.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SID<String>

Gets desktops by machine SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Tag<String>

Get desktops tagged with the given tag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WillShutdownAfterUse<Boolean>

Gets desktops depending on whether they shutdown after use or not.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.SharedDesktop

Get-BrokerSharedDesktop returns an object for each matching shared desktop.

Notes

To compare dates/times, use -Filter and relative comparisons. For more information, see about_Broker_Filtering.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerSharedDesktop -HostingServerName BigServer12*
Get all shared desktops hosted by the hypervisor server BigServer12.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerSharedDesktop -OSType 'Windows XP*' | ft -a MachineName,OSType,OSVersion
List all shared desktops running Windows XP, including the machine name and OS details.

Get-BrokerSite

Sep 10, 2014

Gets the current XenDesktop broker site.

Syntax

```
Get-BrokerSite [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Get-BrokerSite cmdlet gets the current broker site.

The broker site is a top-level, logical representation of the XenDesktop site, from the perspective of the brokering services running within the site. It defines various site-wide default attributes used by the brokering services.

A XenDesktop installation has only a single broker site instance.

---------- BrokerSite Object

The BrokerSite object represents logical representation of the XenDesktop site. It contains the following properties:

-- BaseOU (System.Guid?)

The objectGUID property identifying the base OU in Active Directory used for desktop registrations.

-- BrokerServiceGroupUid (System.Guid)

The Uid for the Broker Service Group.

-- ColorDepth (Citrix.Broker.Admin.SDK.ColorDepth)

The default color depth for new desktop groups.

-- ConfigurationServiceGroupUid (System.Guid?)

The Uid for the Configuration Service Group.

-- ConnectionLeasingEnabled (System.Boolean?)

The indicator for connection leasing active.

-- DesktopGroupIconUid (System.Int32)

The default desktop icon used for new desktop groups.

-- DnsResolutionEnabled (System.Boolean)

The setting to configure whether numeric IP address or the DNS name to be present in the ICA file.

-- LicensedSessionsActive (System.Int32?)

The count of active liscensed session.

-- LicenseEdition (System.String)

The license edition for session brokering.

-- LicenseGraceSessionsRemaining (System.Int32?)

The count of License Grace Session Remaining

-- LicenseModel (Citrix.Broker.Admin.SDK.LicenseModel?)

The licensing model in use. Values can be 'Concurrent' or 'UserDevice'

-- LicenseServerName (System.String)

The DNS for License Server Name

-- LicenseServerPort (System.Int32)

The port for the License Server

-- LicensingBurnIn (System.String)

The date for the license to end in yyyy.MMdd format

-- LicensingBurnInDate (System.DateTime?)

The date for the license to end

-- LicensingGraceHoursLeft (System.Int32?)

The number of grace hours left after license expiry

-- LicensingGracePeriodActive (System.Boolean?)

The indicator for liscensing grace period active

-- LicensingOutOfBoxGracePeriodActive (System.Boolean?)

The indicator for liscensing out of the box grace period active

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

The metadata for this command.

-- Name (System.String)

The name of the site

-- SecureIcaRequired (System.Boolean)

The default SecureICA usage requirements for new desktop groups.

-- TrustRequestsSentToTheXmlServicePort (System.Boolean)

The XML Service trust settings.

Related topics

Set-BrokerSite

Get-BrokerIcon

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Site

Get-BrokerSite returns the single broker site instance.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerSite
Gets the current broker site.

Get-BrokerTag

Sep 10, 2014

Gets one or more tags.

Syntax

Get-BrokerTag [-Uid] <Int32> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerTag [[-Name] <String>] [-Metadata <String>] [-UUID <Guid>] [-DesktopUid <Int32>] [-DesktopGroupUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets tags that match all of the supplied criteria.

---------- BrokerTag Object

The BrokerTag object represents a single instance of a Tag associated to other objects. It contains the following properties:

-- MetadataMap (System.Collections.Generic.Dictionary<string, string>)

The metadata for this command.

-- Name (System.String)

The name of the Tag

-- Uid (System.Int32)

The Uid of the Tag

-- UUID (System.Guid)

The UUID associated to the Tag

Related topics

Add-BrokerTag

New-BrokerTag

Remove-BrokerTag

Rename-BrokerTag

Parameters

-Uid<Int32>

Gets the tag identified by Uid

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets tags that match the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-UUID<Guid>

Gets tags associated with a given UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopUid<Int32>

Gets tags associated with a Desktop.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets tags associated with a desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None Input cannot be piped to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Tag

Returns matching tags.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerTag
Enumerate all tags

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerTag -Uid 5
Get a single specific tag with a Uid of 5.

---------- EXAMPLE 3 ----------

C:\PS> Get-BrokerTag -DesktopUid 1
Get tags associated with Desktop 1.

Get-BrokerUnconfiguredMachine

Sep 10, 2014

Gets machines that have registered but are not yet configured in this site.

Syntax

Get-BrokerUnconfiguredMachine -SID <String> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerUnconfiguredMachine [[-MachineName] <String>] [-AgentVersion <String>] [-ControllerDNSName <String>] [-DNSName <String>] [-FunctionalLevel <FunctionalLevel>] [-LastDeregistrationTime <DateTime>] [-OSType <String>] [-OSVersion <String>] [-SessionSupport <SessionSupport>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieve machines matching the specified criteria, where the machine has registered with a controller in the site but the machine has not yet been configured to be part of the site. If no parameters are specified, this cmdlet enumerates all such machines.

See about_Broker_Filtering for information about advanced filtering options, and about_Broker_Machines for background information about machines.

---------- BrokerUnconfiguredMachine Object

An unconfigured machine is a machine that has registered with the site but is not configured in either a desktop group or a catalog.

-- AgentVersion (System.String)

Version of the Citrix Virtual Delivery Agent (VDA) installed on the unconfigured machine.

-- ControllerDNSName (System.String)

The DNS name of the controller that the unconfigured machine is registered with.

-- DNSName (System.String)

The DNS name of the unconfigured machine.

-- FunctionalLevel (Citrix.Broker.Admin.SDK.FunctionalLevel?)

The functional level of the unconfigured machine. This is determined by the version of the Citrix VDA software installed on the machine.

-- LastDeregistrationTime (System.DateTime?)

The time when the unconfigured machine last deregistered with the Citrix Broker Service.

-- MachineName (System.String)

The machine name of the unconfigured machine in the form domain\machine.

-- OSType (System.String)

The type of operating system installed on the unconfigured machine.

-- OSVersion (System.String)

The version of the operating sysetem installed on the unconfigured machine.

-- SessionSupport (Citrix.Broker.Admin.SDK.SessionSupport?)

The session support of the unconfigured machine. Valid values are:

SingleSession, MultiSession

-- SID (System.String)

Security identifier of the unconfigured machine.

Related topics

Get-BrokerMachine

Parameters

-SID<String>

Gets machines by their machine SID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets machines by their machine name (in the form domain\machine).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AgentVersion<String>

Gets machines with a specific Virtual Desktop Agent version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ControllerDNSName<String>

Gets machines by the DNS name of the controller they are registered with.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets machines by their DNS name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-FunctionalLevel<FunctionalLevel>

Gets machines with a specific FunctionalLevel.

Valid values are L5, L7, L7_6

Required?	false
Default Value	

Accept Pipeline Input?	false

-LastDeregistrationTime<DateTime>

Gets machines by the time that they were last deregistered.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets machines by the type of operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSVersion<String>

Gets machines by the version of the operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSupport<SessionSupport>

Gets machines that have the specified session capability. Values can be:

o SingleSession - Single-session only machine.

o MultiSession - Multi-session capable machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.UnconfiguredMachine

Get-BrokerUnconfiguredMachine returns an object for each matching machine

Notes

It is generally better to compare dates and times using -Filter and relative comparisons. See about_Broker_Filtering and the examples in this topic for more information.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerUnconfiguredMachine -Filter { ControllerDNSName -eq 'Controller1.domain.com' -and OSType -eq 'Windows XP Service Pack 3' }
```

This command returns all unconfigured XP SP3 machines which are registered with the controller called 'Controller1.domain.com'.

Get-BrokerUser

Sep 10, 2014

Gets broker users configured for this site.

Syntax

Get-BrokerUser -SID <String> [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Get-BrokerUser [[-Name] <String>] [-FullName <String>] [-UPN <String>] [-ApplicationUid <Int32>] [-SessionLingerDesktopGroupUid <Int32>] [-SessionPreLaunchDesktopGroupUid <Int32>] [-MachineUid <Int32>] [-PrivateDesktopUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-Property <String[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieve broker users matching the specified criteria. If no parameters are specified this cmdlet enumerates all broker users.

For information about advanced filtering options, see about_Broker_Filtering.

---------- BrokerUser Object

The BrokerUser object represents a single instance of an user. It contains the following properties:

-- FullName (System.String)

The full name of an user

-- Name (System.String)

The name of an user

-- SID (System.String)

The SID of an user

-- UPN (System.String)

The UPN of an user

Related topics

Add-BrokerUser

Remove-BrokerUser

Parameters

-SID<String>

Gets the broker user with the specified SID property value.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Name<String>

Gets the broker user with the specified Name property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-FullName<String>

Gets the broker user with the specified FullName property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UPN<String>

Gets the broker user with the specified UPN property value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationUid<Int32>

Gets broker users associated with the application with the specified Uid.

Required?	false

Default Value	
Accept Pipeline Input?	false

-SessionLingerDesktopGroupUid<Int32>

Gets broker users associated with the desktop group session linger settings with the specified Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionPreLaunchDesktopGroupUid<Int32>

Gets broker users associated with the desktop group session pre-launch settings with the specified Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineUid<Int32>

Gets broker users associated with the broker machine with the specified Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PrivateDesktopUid<Int32>

Gets broker users associated with the private desktop with the specified Uid.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false

Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.User

Get-BrokerUser returns an object for each matching broker user.

Examples

---------- EXAMPLE 1 ----------

```
Get-BrokerUser DOMAIN7\*
```

Get all broker user objects with names matching the supplied pattern

---------- EXAMPLE 2 ----------

```
$pdt = Get-BrokerPrivateDesktop DOMAIN\MACHINENAME\n
        Get-BrokerUser -PrivateDesktopUid $pdt.Uid
```

Get all broker user objects added to the specified private desktop

Group-BrokerDesktop

Sep 10, 2014

Groups and counts desktops with the same value for a specified property.

Syntax

Group-BrokerDesktop [-Uid] <Int32> -Property <String> [-AdminAddress <String>] [<CommonParameters>]

Group-BrokerDesktop -Property <String> [[-MachineName] <String>] [-AgentVersion <String>] [-ApplicationInUse <String>] [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-AssociatedUserFullName <String>] [-AssociatedUserName <String>] [-AssociatedUserUPN <String>] [-AutonomouslyBrokered <Boolean>] [-CatalogName <String>] [-CatalogUid <Int32>] [-ClientAddress <String>] [-ClientName <String>] [-ClientVersion <String>] [-ColorDepth <ColorDepth>] [-ConnectedViaHostName <String>] [-ConnectedViaIP <String>] [-ControllerDNSName <String>] [-DeliveryType <DeliveryType>] [-Description <String>] [-DesktopCondition <String>] [-DesktopGroupName <String>] [-DesktopGroupUid <Int32>] [-DesktopKind <DesktopKind>] [-DeviceId <String>] [-DNSName <String>] [-FunctionalLevel <FunctionalLevel>] [-HardwareId <String>] [-HostedMachineId <String>] [-HostedMachineName <String>] [-HostingServerName <String>] [-HypervisorConnectionName <String>] [-HypervisorConnectionUid <Int32>] [-IconUid <Int32>] [-ImageOutOfDate <Boolean>] [-InMaintenanceMode <Boolean>] [-IPAddress <String>] [-IsAssigned <Boolean>] [-IsPhysical <Boolean>] [-LastConnectionFailure <ConnectionFailureReason>] [-LastConnectionTime <DateTime>] [-LastConnectionUser <String>] [-LastDeregistrationReason <DeregistrationReason>] [-LastDeregistrationTime <DateTime>] [-LastErrorReason <String>] [-LastErrorTime <DateTime>] [-LastHostingUpdateTime <DateTime>] [-LaunchedViaHostName <String>] [-LaunchedViaIP <String>] [-MachineInternalState <MachineInternalState>] [-MachineUid <Int32>] [-OSType <String>] [-OSVersion <String>] [-PersistUserChanges <PersistUserChanges>] [-PowerActionPending <Boolean>] [-PowerState <PowerState>] [-Protocol <String>] [-ProvisioningType <ProvisioningType>] [-PublishedApplication <String>] [-PublishedName <String>] [-PvdStage <PvdStage>] [-RegistrationState <RegistrationState>] [-SecureIcaActive <Boolean>] [-SecureIcaRequired <Boolean>] [-SessionHidden <Boolean>] [-SessionId <Int32>] [-SessionState <SessionState>] [-SessionStateChangeTime <DateTime>] [-SessionUid <Int64>] [-SessionUserName <String>] [-SessionUserSID <String>] [-SID <String>] [-SmartAccessTag <String>] [-StartTime <DateTime>] [-SummaryState <DesktopSummaryState>] [-Tag <String>] [-WillShutdownAfterUse <Boolean>] [-ApplicationUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

This cmdlet is now deprecated, please use Group-BrokerMachine.

Filters desktops using the specified criteria, then groups and counts matching desktops with the same value for a particular property. The number of desktops in the group, and the property value for the group, is output. For example:

C:\PS> Group-BrokerDesktop -Property SummaryState

Count Name

----- ----

43 Available

17 InUse

3 Disconnected

Filtering supports the same options as the Get-BrokerDesktop cmdlet, and allows filtering on both desktop and session properties.

Group-BrokerDesktop is similar to the standard PowerShell Group-Object, but is faster than piping the output of Get-BrokerDesktop into Group-Object when working with many desktops.

Note that all session information properties for multi-session desktops is always $null, this means that is is not possible to group these desktops by session information using this command. Use Get-BrokerSession to get information on all current sessions.

Also note that the MaxRecordCount, ReturnTotalRecordCount, Skip, and SortBy parameters apply to GroupInfo records output rather than the filtered desktops.

Related topics

Get-BrokerDesktop

Group-Object

Parameters

-Uid<Int32>

Gets desktops with a specific UID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Property<String>

Selects the property by which matching desktops are grouped.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets desktops with a specific machine name (in the form 'domain\machine').

Required?	false
Default Value	
Accept Pipeline Input?	false

-AgentVersion<String>

Gets desktops with a specific Citrix Virtual Delivery Agent version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationInUse<String>

Gets desktops running a specified published application (identified by browser name).

String comparisons are case-insensitive.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedClientName<String>

Gets desktops assigned to a specific client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedIPAddress<String>

Gets desktops assigned to a specific IP address.q

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserFullName<String>

Gets desktops with an associated user identified by their full name (usually in the form 'first-name last-name').

Associated users are the current user for shared desktops, and the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserName<String>

Gets desktops with an associated user identified by their user name (in the form 'domain\user').

Associated users are the current user for shared desktops, and the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserUPN<String>

Gets desktops with an associated user identified by their User Principle Name (in the form 'user@domain').

Associated users are the current user for shared desktops, and the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AutonomouslyBrokered<Boolean>

Gets desktops according to whether their current session is autonomously brokered or not. Autonomously brokered sessions are HDX sessions established by direct connection without being brokered.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogName<String>

Gets desktops from the catalog with the specific name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogUid<Int32>

Gets desktops from a catalog with a specific UID.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ClientAddress<String>

Gets desktops with a specific client IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientName<String>

Gets desktops with a specific client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientVersion<String>

Gets desktops with a specific client version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Gets desktops configured with a specific color depth.

Valid values are FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectedViaHostName<String>

Gets desktops with a specific host name of the incoming connection. This is usually a proxy or Citrix Access Gateway server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectedViaIP<String>

Gets desktops with a specific IP address of the incoming connection.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ControllerDNSName<String>

Gets desktops with a specific DNS name of the controller they are registered with.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeliveryType<DeliveryType>

Gets desktops of a particular delivery type.

Valid values are AppsOnly, DesktopsOnly, DesktopsAndApps

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Get desktops with a specific description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopCondition<String>

Gets desktop with an outstanding desktop condition condition.

Valid values are:

o CPU: Indicates the machine has high CPU usage

o ICALatency: Indicates the network latency is high

o UPMLogonTime: Indicates that the profile load time was high

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets desktops from a desktop group with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets desktops from a desktop group with the specified UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopKind<DesktopKind>

Deprecated: Use AllocationType parameter.

Gets desktops of a particular kind.

Valid values are Private, Shared.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeviceId<String>

Gets desktops with a specific client device ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Get desktops with a specific DNS name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-FunctionalLevel<FunctionalLevel>

Gets desktops with a specific FunctionalLevel.

Valid values are L5, L7, L7_6

Required?	false
Default Value	
Accept Pipeline Input?	false

-HardwareId<String>

Gets desktops with a specific client hardware ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineId<String>

Gets desktops with a specific machine ID known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets desktops with a specific machine name known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostingServerName<String>

Gets desktops with a specific name of the hosting hypervisor server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionName<String>

Gets desktops with a specific name of the hosting hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets desktops with a specific UID of the hosting hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Gets desktops with a specific configured icon. Note that desktops with a null IconUid use the icon of the desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ImageOutOfDate<Boolean>

Gets desktops if they have an ImageOutOfDate flag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Gets desktops with a specific InMaintenanceMode setting.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IPAddress<String>

Gets desktops with a specific IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsAssigned<Boolean>

Gets desktops according to whether they are assigned or not. Desktops may be assigned to one or more users or groups, a client IP address or a client endpoint name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsPhysical<Boolean>

Specifies if machines in the catalog can be power managed by the Citrix Broker Service. Where the power state of the machine cannot be controlled, specify $true, otherwise $false. Can only be specified together with a provisioning type of Pvs or Manual, or if used with the deprecated CatalogKind parameter only with Pvs or PvsPvd catalog kinds.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastConnectionFailure<ConnectionFailureReason>

Gets desktops with a specific reason for the last recorded connection failure. This value is None if the last connection was successful or if there has been no attempt to connect to the desktop yet.

Valid values are None, SessionPreparation, RegistrationTimeout, ConnectionTimeout, Licensing, Ticketing, and Other.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastConnectionTime<DateTime>

Gets desktops that last connected at a specific time. This is the time that the broker detected that the connection attempt either succeeded or failed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastConnectionUser<String>

Gets desktops where a specific user name last attempted a connection (in the form 'domain\user').

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationReason<DeregistrationReason>

Gets desktops whose broker last recorded a specific deregistration reason.

Valid values are $null, AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationTime<DateTime>

Gets desktops that were last deregistered by a specific time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastErrorReason<String>

Gets desktops with the specified last error reason.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastErrorTime<DateTime>

Gets desktops with the specified last error time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastHostingUpdateTime<DateTime>

Gets desktops with a specific time that the hosting information was last updated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LaunchedViaHostName<String>

Gets desktops with a specific host name of the StoreFront server from which the user launched the session.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LaunchedViaIP<String>

Gets desktops with a specific IP address of the StoreFront server from which the user launched the session.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineInternalState<MachineInternalState>

Gets desktops with the specified internal machine state.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineUid<Int32>

Gets desktops with a specific machine UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets desktops by the type of operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSVersion<String>

Gets desktops by the version of the operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PersistUserChanges<PersistUserChanges>

Gets desktops by the location where the user changes are persisted.

o OnLocal - User changes are persisted locally.

o Discard - User changes are discarded.

o OnPvd - User changes are persisted on the Pvd.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerActionPending<Boolean>

Gets desktops with a specific power action pending state.

Valid values are $true or $false.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerState<PowerState>

Gets desktops with a specific power state.

Valid values are Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Protocol<String>

Gets desktops with connections using a specific protocol, for example HDX, RDP, or Console.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningType<ProvisioningType>

Specifies the provisioning type for the catalog. Values can be:

o Manual - No provisioning.

o PVS - Machine provisioned by PVS (machine may be physical, blade, VM,...).

o MCS - Machine provisioned by MCS (machine must be VM).

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedApplication<String>

Gets desktops with a specific application published on them (identified by its browser name).

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Gets desktops with a specific published name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdStage<PvdStage>

Gets machines with a specific personal vDisk stage.

Valid values are None, Requested, Starting, Working and Failed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RegistrationState<RegistrationState>

Gets desktops with a specific registration state.

Valid values are Unregistered, Initializing, Registered and AgentError.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaActive<Boolean>

Gets desktops depending on whether the current session uses SecureICA or not.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Gets desktops configured with a particular SecureIcaRequired setting. Note that the desktop setting of $null indicates that the desktop group value is used.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionHidden<Boolean>

Gets desktops by whether their sessions are hidden or not. Hidden sessions are treated as though they do not exist when launching sessions; a hidden session cannot be reconnected to, but a new session may be launched using the same entitlement.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionId<Int32>

Deprecated.

Gets desktops by session ID, a unique identifier that Remote Desktop Services uses to track the session but it is only unique on that machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionState<SessionState>

Gets desktops with a specific session state.

Valid values are $null, Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession, and Unknown.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionStateChangeTime<DateTime>

Gets desktops whose sessions last changed state at a specific time.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUid<Int64>

Gets desktops with a specific session UID ($null for no session).

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUserName<String>

Gets desktops with a specific user name for the current session (in the form 'domain\user').

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUserSID<String>

Gets desktops with a specific SID of the current session user.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SID<String>

Gets desktops with a specific machine SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SmartAccessTag<String>

Gets desktops where the session has the specific SmartAccess tag.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartTime<DateTime>

Gets desktops with a specific session start time.

Session properties are always null for multi-session desktops.

Required?	false
Default Value	

Accept Pipeline Input?	false

-SummaryState<DesktopSummaryState>

Gets desktops with a specific summary state.

Valid values are Off, Unregistered, Available, Disconnected, and InUse.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Tag<String>

Gets desktops with a specific tag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WillShutdownAfterUse<Boolean>

Gets desktops depending on whether they shut down after use or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationUid<Int32>

Gets desktops with a specific published application (identified by its UID).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250

Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.GroupInfo

Each GroupInfo object represents one group, and contains the following properties:

-- Count: The count of desktops in this group.

-- Name: The value of the property the desktops were grouped by (as a string).

If you do not specify -SortBy, groups are sorted with the largest count first.

Notes

To compare dates or times, use -Filter and relative comparisons. For more information, see about_Broker_Filtering and the examples.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Group-BrokerDesktop -Property SummaryState -DesktopGroupName dg1
```

Group desktops from the dg1 group by summary state.

---------- EXAMPLE 2 ----------

C:\PS> Group-BrokerDesktop -Property LastConnectionFailure -Filter { LastConnectionFailure -ne "None" -and LastConnectionTime -ge '-7' } -MaxRecordCount 1
For desktops where the last connection attempt failed, list the most common reason for failure, ignoring connections that failed over a week ago.

---------- EXAMPLE 3 ----------

C:\PS> Group-BrokerDesktop -Property HostingServerName -DesktopCondition ICALatency -SortBy Name
List alphabetically the hypervisor servers hosting desktops that are currently experiencing high network latency.

Group-BrokerMachine

Sep 10, 2014

Groups and counts machines with the same value for a specified property.

Syntax

Group-BrokerMachine [-Uid] <Int32> -Property <String> [-AdminAddress <String>] [<CommonParameters>]

Group-BrokerMachine -Property <String> [[-MachineName] <String>] [-AgentVersion <String>] [-AllocationType <AllocationType>] [-ApplicationInUse <String>] [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-AssociatedUserFullName <String>] [-AssociatedUserName <String>] [-AssociatedUserSID <String>] [-AssociatedUserUPN <String>] [-BrowserName <String>] [-CatalogName <String>] [-CatalogUid <Int32>] [-CatalogUUID <Guid>] [-ColorDepth <ColorDepth>] [-ControllerDNSName <String>] [-DeliveryType <DeliveryType>] [-Description <String>] [-DesktopCondition <String>] [-DesktopGroupName <String>] [-DesktopGroupUid <Int32>] [-DesktopGroupUUID <Guid>] [-DesktopKind <DesktopKind>] [-DesktopUid <Int32>] [-DNSName <String>] [-FaultState <MachineFaultState>] [-FunctionalLevel <FunctionalLevel>] [-HostedMachineId <String>] [-HostedMachineName <String>] [-HostingServerName <String>] [-HypervisorConnectionName <String>] [-HypervisorConnectionUid <Int32>] [-HypHypervisorConnectionUid <Guid>] [-IconUid <Int32>] [-ImageOutOfDate <Boolean>] [-InMaintenanceMode <Boolean>] [-IPAddress <String>] [-IsAssigned <Boolean>] [-IsPhysical <Boolean>] [-LastConnectionFailure <ConnectionFailureReason>] [-LastConnectionTime <DateTime>] [-LastConnectionUser <String>] [-LastDeregistrationReason <DeregistrationReason>] [-LastDeregistrationTime <DateTime>] [-LastErrorReason <String>] [-LastErrorTime <DateTime>] [-LastHostingUpdateTime <DateTime>] [-LastPvdErrorReason <String>] [-LastPvdErrorTime <DateTime>] [-LoadIndex <Int32>] [-MachineInternalState <MachineInternalState>] [-Metadata <String>] [-OSType <String>] [-OSVersion <String>] [-PersistUserChanges <PersistUserChanges>] [-PowerActionPending <Boolean>] [-PowerState <PowerState>] [-ProvisioningType <ProvisioningType>] [-PublishedApplication <String>] [-PublishedName <String>] [-PvdEstimatedCompletionTime <DateTime>] [-PvdPercentDone <Int32>] [-PvdStage <PvdStage>] [-PvdUpdateStartTime <DateTime>] [-RegistrationState <RegistrationState>] [-ScheduledReboot <ScheduledReboot>] [-SecureIcaRequired <Boolean>] [-SessionAutonomouslyBrokered <Boolean>] [-SessionClientAddress <String>] [-SessionClientName <String>] [-SessionClientVersion <String>] [-SessionConnectedViaHostName <String>] [-SessionConnectedViaIP <String>] [-SessionCount <Int32>] [-SessionDeviceId <String>] [-SessionHardwareId <String>] [-SessionHidden <Boolean>] [-SessionKey <Guid>] [-SessionLaunchedViaHostName <String>] [-SessionLaunchedViaIP <String>] [-SessionProtocol <String>] [-SessionSecureIcaActive <Boolean>] [-SessionsEstablished <Int32>] [-SessionSmartAccessTag <String>] [-SessionsPending <Int32>] [-SessionStartTime <DateTime>] [-SessionState <SessionState>] [-SessionStateChangeTime <DateTime>] [-SessionSupport <SessionSupport>] [-SessionType <SessionType>] [-SessionUid <Int64>] [-SessionUserName <String>] [-SessionUserSID <String>] [-SID <String>] [-SummaryState <DesktopSummaryState>] [-SupportedPowerActions <String[]>] [-Tag <String>] [-UUID <Guid>] [-VMToolsState <VMToolsState>] [-WillShutdownAfterUse <Boolean>] [-WindowsConnectionSetting <WindowsConnectionSetting>] [-AssignedUserSID <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Filters machines using the specified criteria, then groups and counts matching machines with the same value for a particular property. The number of machines in the group, and the property value for the group, is output. For example:

C:\PS> Group-BrokerMachine -Property SummaryState

Count Name

----- ----

43 Available

17 InUse

3 Disconnected

Filtering supports the same options as the Get-BrokerMachine cmdlet, and allows filtering on both machine and session properties.

Group-BrokerMachine is similar to the standard PowerShell Group-Object, but is faster than piping the output of Get-BrokerMachine into Group-Object when working with many machines.

Note that the MaxRecordCount, ReturnTotalRecordCount, Skip, and SortBy parameters apply to GroupInfo records output rather than the filtered machines.

Related topics

Get-BrokerMachine

Group-Object

Parameters

-Uid<Int32>

Gets a machine with a specific UID.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Property<String>

Selects the property by which matching machines are grouped.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets machines with a specific machine name (in the form domain\machine).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AgentVersion<String>

Gets machines with a specific Virtual Delivery Agent version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AllocationType<AllocationType>

Gets machines from catalogs with the specified allocation type.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationInUse<String>

Gets machines running a specified published application. String comparisons are case-insensitive.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedClientName<String>

Gets machines that have been assigned to the specific client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedIPAddress<String>

Gets machines that have been assigned to the specific client IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserFullName<String>

Gets machines with an associated user identified by their full name (usually 'first-name last-name').

Associated users are all current users of a desktop, plus the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserName<String>

Gets machines with an associated user identified by their user name (in the form 'domain\user').

Associated users are all current users of a desktop, plus the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserSID<String>

Gets machines with an associated user identified by their Windows SID.

Associated users are all current users of a desktop, plus the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssociatedUserUPN<String>

Gets machines with an associated user identified by their User Principle Name (in the form 'user@domain').

Associated users are all current users of a desktop, plus the assigned users for private desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrowserName<String>

Gets assigned machines backing desktop resources that have browser names matching the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogName<String>

Gets machines from the catalog with the specific name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogUid<Int32>

Gets machines from the catalog with the specific UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogUUID<Guid>

Gets machines from the catalog with the specific UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Gets machines configured with a specific color depth.

Valid values are FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ControllerDNSName<String>

Gets machines by the DNS name of the controller they are registered with.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeliveryType<DeliveryType>

Gets machines of a particular delivery type.

Valid values are AppsOnly, DesktopsOnly, DesktopsAndApps

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Get machines by description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopCondition<String>

Gets machines with an outstanding desktop condition.

Valid values are:

o CPU: Indicates the machine has high CPU usage

o ICALatency: Indicates the network latency is high

o UPMLogonTime: Indicates that the profile load time was high

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets machines from a desktop group with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets machines from a desktop group with a specific UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUUID<Guid>

Gets machines from a desktop group with a specific UUID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopKind<DesktopKind>

Deprecated: Use AllocationType parameter.

Gets machines of a particular kind.

Valid values are Private, Shared.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopUid<Int32>

Gets the machine that corresponds to the desktop with the specific UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets machines with the specific DNS name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-FaultState<MachineFaultState>

Gets machines currently in the specified fault state.

Required?	false
Default Value	
Accept Pipeline Input?	false

-FunctionalLevel<FunctionalLevel>

Gets machines with a specific FunctionalLevel.

Valid values are L5, L7, L7_6

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineId<String>

Gets machines with the specific machine ID known to the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets machines with the specific machine name known to the hypervisor.

Required?	false

Default Value	
Accept Pipeline Input?	false

-HostingServerName<String>

Gets machines by the name of the hosting hypervisor server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionName<String>

Gets machines with the specific name of the hypervisor connection hosting them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

Gets machines with the specific UID of the hypervisor connection hosting them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypHypervisorConnectionUid<Guid>

Gets machines with the specific UUID of the hypervisor connection hosting them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Gets machines by configured icon. Note that machines with a null IconUid use the icon of the desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ImageOutOfDate<Boolean>

Gets machines depending on whether their disk image is out of date or not (for machines provisioned using MCS only).

Required?	false
Default Value	

Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Gets machines by whether they are in maintenance mode or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IPAddress<String>

Gets machines with a specific IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsAssigned<Boolean>

Gets machines according to whether they are assigned or not. Machines may be assigned to one or more users or groups, a client IP address or a client endpoint name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsPhysical<Boolean>

Gets machines according to whether they can be power managed by XenDesktop or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastConnectionFailure<ConnectionFailureReason>

Gets machines with a specific reason for the last recorded connection failure. This value is None if the last connection was successful or if there has been no attempt to connect to the machine yet.

Valid values are None, SessionPreparation, RegistrationTimeout, ConnectionTimeout, Licensing, Ticketing, and Other.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastConnectionTime<DateTime>

Gets machines to which a user session connection occurred at a specific time. This is the time that the broker detected that the connection attempt either succeeded or failed.

Required?	false
Default Value	

Accept Pipeline Input?	false

-LastConnectionUser<String>

Gets machines where a specific user name last attempted a connection (in the form 'domain\user').

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationReason<DeregistrationReason>

Gets machines whose broker last recorded a specific deregistration reason.

Valid values are $null, AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError and BrokerRegistrationLimitReached.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastDeregistrationTime<DateTime>

Gets machines by the time that they were last deregistered.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastErrorReason<String>

Gets machines with the specified last error reason.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastErrorTime<DateTime>

Gets machines with the specified last error time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastHostingUpdateTime<DateTime>

Gets machines with a specific time that the hosting information was last updated.

Required?	false
Default Value	

Accept Pipeline Input?	false

-LastPvdErrorReason<String>

Gets machines with the specified last Personal vDisk preparation error reason.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LastPvdErrorTime<DateTime>

Gets machines with the specified last Personal vDisk preparation error time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoadIndex<Int32>

Gets machines by their current load index.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineInternalState<MachineInternalState>

Gets machines with the specified internal state.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets machines by the type of operating system they are running.

Required?	false
Default Value	

Accept Pipeline Input?	false

-OSVersion<String>

Gets machines by the version of the operating system they are running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PersistUserChanges<PersistUserChanges>

Gets machines according to the location where user changes are persisted. Values can be:

o OnLocal - User changes are persisted locally.

o Discard - User changes are discarded.

o OnPvd - User changes are persisted on the Pvd.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerActionPending<Boolean>

Gets machines depending on whether a power action is pending or not.

Valid values are $true or $false.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PowerState<PowerState>

Gets machines with a specific power state.

Valid values are Unmanaged, Unknown, Unavailable, Off, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningType<ProvisioningType>

Specifies the provisioning type for the catalog. Values can be:

o Manual - No provisioning.

o PVS - Machine provisioned by PVS (machine may be physical, blade, VM,...).

o MCS - Machine provisioned by MCS (machine must be VM).

Required?	false
Default Value	

Accept Pipeline Input?	false

-PublishedApplication<String>

Gets machines with a specific application published to them (identified by its browser name).

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Gets desktops with a specific published name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdEstimatedCompletionTime<DateTime>

If preparation of the Personal vDisk is currently in progress for this machine, this reports an estimation of the time at which the process will be complete.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdPercentDone<Int32>

Gets machines a specific percentage through the Personal vDisk preparation process.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdStage<PvdStage>

Gets machines at a specific personal vDisk stage.

Valid values are None, Requested, Starting, Working and Failed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvdUpdateStartTime<DateTime>

If preparation of the Personal vDisk is currently in progress for this machine, this reports when the update process began.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RegistrationState<RegistrationState>

Gets machines in a specific registration state.

Valid values are Unregistered, Initializing, Registered, and AgentError.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScheduledReboot<ScheduledReboot>

Gets machines according to their current status with respect to any scheduled reboots (for either scheduled desktop group reboots or image rollout purposes). Valid values are:

o None - No reboot currently scheduled.

o Pending - Reboot scheduled but machine still available for use.

o Draining - Reboot scheduled. New logons are disabled, but reconnections to existing sessions are allowed.

o InProgress - Machine is actively being rebooted.

o Natural - Natural reboot in progress. Machine is awaiting a restart.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Gets machines configured with a particular SecureIcaRequired setting. Note that the machine setting of $null indicates that the desktop group value is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionAutonomouslyBrokered<Boolean>

Gets machines according to whether their current session is autonomously brokered or not. Autonomously brokered sessions are HDX sessions established by direct connection without being brokered.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionClientAddress<String>

Gets machines with a specific client IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionClientName<String>

Gets machines with a specific client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionClientVersion<String>

Gets machines with a specific client version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionConnectedViaHostName<String>

Gets machines with a specific host name of the incoming connection. This is usually a proxy or Citrix Access Gateway server.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionConnectedViaIP<String>

Gets machines with a specific IP address of the incoming connection.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionCount<Int32>

Gets machines according to the total number of both pending and established user sessions on the machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionDeviceId<String>

Gets machines with a specific client device ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionHardwareId<String>

Gets machines with a specific client hardware ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionHidden<Boolean>

Gets machines by whether their sessions are hidden or not. Hidden sessions are treated as though they do not exist when launching sessions using XenDesktop; a hidden session cannot be reconnected to, but a new session may be launched using the same entitlement.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionKey<Guid>

Gets machine running the session with the specified unique key.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionLaunchedViaHostName<String>

Gets machines with a specific host name of the Web Interface server from which the user launched the session.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionLaunchedViaIP<String>

Gets machines with a specific IP address of the Web Interface server from which the user launched the session.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionProtocol<String>

Gets machines with connections using a specific protocol, for example HDX, RDP, or Console.

Required?	false
Default Value	

Accept Pipeline Input?	false

-SessionSecureIcaActive<Boolean>

Gets machines depending on whether the current session uses SecureICA or not.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionsEstablished<Int32>

Gets machines according to the number of established user sessions present on the machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSmartAccessTag<String>

Gets session machines where the session has the specific SmartAccess tag.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionsPending<Int32>

Get machines according to the number of pending user sessions for the machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionStartTime<DateTime>

Gets machines with a specific session start time.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionState<SessionState>

Gets machines with a specific session state.

Valid values are $null, Other, PreparingSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession, and Unknown.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionStateChangeTime<DateTime>

Gets machines whose sessions last changed state at a specific time.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSupport<SessionSupport>

Gets machines that have the specified session capability. Values can be:

o SingleSession - Single-session only machine.

o MultiSession - Multi-session capable machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionType<SessionType>

Gets machines with a specific session state.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUid<Int64>

Gets single-session machines with a specific session UID ($null for no session).

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionUserName<String>

Gets machines with a specific user name for the current session (in the form 'domain\user').

Session properties are always null for multi-session machines.

Required?	false
Default Value	

Accept Pipeline Input?	false

-SessionUserSID<String>

Gets machines with a specific SID of the current session user.

Session properties are always null for multi-session machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SID<String>

Gets machines with a specific machine SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SummaryState<DesktopSummaryState>

Gets machines with a specific summary state.

Valid values are Off, Unregistered, Available, Disconnected, and InUse.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SupportedPowerActions<String[]>

A list of power actions supported by this machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Tag<String>

Gets machines where the session has the given SmartAccess tag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UUID<Guid>

Gets machines with the specified value of UUID.

Required?	false
Default Value	

Accept Pipeline Input?	false

-VMToolsState<VMToolsState>

Gets machines with a specific VM tools state.

Valid values are NotPresent, Unknown, NotStarted, and Running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WillShutdownAfterUse<Boolean>

Gets machines depending on whether they shut down after use or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WindowsConnectionSetting<WindowsConnectionSetting>

Gets machines according to their current Windows connection setting (logon mode). Valid values are:

o LogonEnabled - All logons are enabled.

o Draining - New logons are disabled, but reconnections to existing sessions are allowed.

o DrainingUntilRestart - Same as Draining, but setting reverts to LogonEnabled when machine next restarts.

o LogonDisabled - All logons and reconnections are disabled.

This is a Windows setting and is not controlled by XenDesktop. It applies only to multi-session machines; for single-session machines its value is always LogonEnabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedUserSID<String>

Gets machines with the specific SID of the user to whom the desktop is assigned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.GroupInfo

Each GroupInfo object represents one group, and contains the following properties:

-- Count: The count of machines in this group.

-- Name: The value of the property the machines were grouped by (as a string).

If you do not specify -SortBy, groups are sorted with the largest count first.

Notes

To compare dates or times, use -Filter and relative comparisons. For more information, see about_Broker_Filtering and the examples.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Group-BrokerMachine -Property SummaryState -DesktopGroupName dg1
Group machines from the dg1 group by summary state.

---------- EXAMPLE 2 ----------

C:\PS> Group-BrokerMachine -Property LastConnectionFailure -Filter { LastConnectionFailure -ne "None" -and LastConnectionTime -ge '-7' } -MaxRecordCount 1
For machines where the last connection attempt failed, list the most common reason for failure, ignoring connections that failed over a week ago.

---------- EXAMPLE 3 ----------

C:\PS> Group-BrokerMachine -Property HostingServerName -DesktopCondition ICALatency -SortBy Name
List alphabetically the hypervisor servers hosting machines that are currently experiencing high network latency.

Group-BrokerSession

Sep 10, 2014

Groups and counts sessions with the same value for a specified property.

Syntax

Group-BrokerSession [-Uid] <Int64> -Property <String> [-AdminAddress <String>] [<CommonParameters>]

Group-BrokerSession -Property <String> [[-SessionKey] <Guid>] [-AgentVersion <String>] [-ApplicationInUse <String>] [-AppState <SessionAppState>] [-AppStateLastChangeTime <DateTime>] [-AutonomouslyBrokered <Boolean>] [-BrokeringDuration <Int32>] [-BrokeringTime <DateTime>] [-BrokeringUserName <String>] [-BrokeringUserSID <String>] [-CatalogName <String>] [-ClientAddress <String>] [-ClientName <String>] [-ClientPlatform <String>] [-ClientProductId <Int32>] [-ClientVersion <String>] [-ConnectedViaHostName <String>] [-ConnectedViaIP <String>] [-ConnectionMode <ConnectionMode>] [-ControllerDNSName <String>] [-DesktopGroupName <String>] [-DesktopGroupUid <Int32>] [-DesktopKind <DesktopKind>] [-DesktopSID <String>] [-DesktopUid <Int32>] [-DeviceId <String>] [-DNSName <String>] [-EstablishmentDuration <Int32>] [-EstablishmentTime <DateTime>] [-HardwareId <String>] [-Hidden <Boolean>] [-HostedMachineName <String>] [-HostingServerName <String>] [-HypervisorConnectionName <String>] [-ImageOutOfDate <Boolean>] [-InMaintenanceMode <Boolean>] [-IPAddress <String>] [-IsAnonymousUser <Boolean>] [-IsPhysical <Boolean>] [-LaunchedViaHostName <String>] [-LaunchedViaIP <String>] [-LogoffInProgress <Boolean>] [-LogonInProgress <Boolean>] [-MachineName <String>] [-MachineSummaryState <DesktopSummaryState>] [-MachineUid <Int32>] [-Metadata <String>] [-OSType <String>] [-PersistUserChanges <PersistUserChanges>] [-PowerState <PowerState>] [-Protocol <String>] [-ProvisioningType <ProvisioningType>] [-ReceiverIPAddress <String>] [-ReceiverName <String>] [-SecureIcaActive <Boolean>] [-SessionId <Int32>] [-SessionState <SessionState>] [-SessionStateChangeTime <DateTime>] [-SessionSupport <SessionSupport>] [-SessionType <SessionType>] [-StartTime <DateTime>] [-UntrustedUserName <String>] [-UserFullName <String>] [-UserName <String>] [-UserSID <String>] [-UserUPN <String>] [-ApplicationUid <Int32>] [-SharedDesktopUid <Int32>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Filters sessions using the specified criteria, then groups and counts matching sessions with the same value for a particular property. The number of sessions in the group, and the property value for the group, is output. For example:

C:\PS> Group-BrokerSession -Property SessionState

Count Name

----- ----

43 Active

17 NonBrokeredSession

3 Disconnected

Filtering supports the same options as the Get-BrokerSession cmdlet, and allows filtering on both machine and session properties.

Group-BrokerSession is similar to the standard PowerShell Group-Object, but is faster than piping the output of Get-BrokerSession into Group-Object when working with many machines.

Note that the MaxRecordCount, ReturnTotalRecordCount, Skip, and SortBy parameters apply to GroupInfo records output rather than the filtered sessions.

Related topics

Get-BrokerSession

Group-Object

Parameters

-Uid<Int64>

Get session by its Uid.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Property<String>

Selects the property by which matching sessions are grouped.

Required?	true
Default Value	
Accept Pipeline Input?	false

-SessionKey<Guid>

Gets session having the specified unique key.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AgentVersion<String>

Gets sessions with a specific Virtual Desktop Agent version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationInUse<String>

Gets sessions running specific applications (identified by their SDK Name property).

Required?	false
Default Value	
Accept Pipeline Input?	false

-AppState<SessionAppState>

Get sessions by their app state.

Valid values are PreLogon, PreLaunched, Active, Desktop, Lingering and NoApps.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AppStateLastChangeTime<DateTime>

Get sessions by their app state change time.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AutonomouslyBrokered<Boolean>

Gets sessions according to whether they are autonomously brokered or not. Autonomously brokered sessions are HDX sessions established by direct connection without being brokered.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringDuration<Int32>

Gets session with a specific time taken to broker. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringTime<DateTime>

Get sessions brokered at a specific time. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringUserName<String>

Get sessions by brokering user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-BrokeringUserSID<String>

Get sessions by brokering user SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CatalogName<String>

Gets sessions on machines from a specific catalog name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientAddress<String>

Get sessions by client IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientName<String>

Get sessions by client name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientPlatform<String>

Get sessions by client platform.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientProductId<Int32>

Get sessions by client product ID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ClientVersion<String>

Get sessions by client version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectedViaHostName<String>

Get sessions by host name of the incoming connection. This is usually a proxy or Citrix Access Gateway server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectedViaIP<String>

Get sessions by IP address of the incoming connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectionMode<ConnectionMode>

Gets sessions by the way in which the most recent connection to the session was established.

Valid modes are Brokered, Unbrokered, LeasedConnection, VdaHighAvailabilityMode, ThirdPartyBroker, and ThirdPartyBrokerWithLicensing.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ControllerDNSName<String>

Gets sessions that are hosted on machines which are registered with a specific controller.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupName<String>

Gets sessions from a desktop group with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupUid<Int32>

Gets sessions from a desktop group with the specified UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopKind<DesktopKind>

Gets sessions on a desktop of a particular kind.

Valid values are Private and Shared.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopSID<String>

Get sessions by desktop SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopUid<Int32>

Get sessions by desktop Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeviceId<String>

Get sessions by client device id.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DNSName<String>

Gets sessions by their machine's DNS name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EstablishmentDuration<Int32>

Gets sessions which took a specific time to establish. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EstablishmentTime<DateTime>

Gets sessions which became established at a particular time. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HardwareId<String>

Get sessions by client hardware id.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Hidden<Boolean>

Get sessions by whether they are hidden or not. Hidden sessions are treated as though they do not exist when brokering sessions; a hidden session cannot be reconnected to, but a new session may be launched using the same entitlement.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineName<String>

Gets sessions by their machine's name as known to its hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostingServerName<String>

Gets sessions hosted by a machine with a specific name of the hosting hypervisor server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HypervisorConnectionName<String>

Gets sessions hosted by a machine with a specific name of the hosting hypervisor connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ImageOutOfDate<Boolean>

Gets sessions hosted by a machine with a specific ImageOutOfDate setting.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Gets sessions hosted by a machine with a specific InMaintenanceMode setting.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IPAddress<String>

Gets sessions hosted by a machine with a specific IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsAnonymousUser<Boolean>

Gets sessions depending on whether they were established anonymously ($true) or not ($false). An anonymous session is established without user credentials and a temporary local user account is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsPhysical<Boolean>

Gets sessions hosted on machines where the flag indicating if the machine can be power managed by the Citrix Broker Service matches the requested value. Where the power state of the machine cannot be controlled, specify $true, otherwise $false.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LaunchedViaHostName<String>

Get sessions by the host name of the Web Interface server from which a user launches a session.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LaunchedViaIP<String>

Get sessions by the IP address of the Web Interface server from which a user launches a session.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LogoffInProgress<Boolean>

Gets sessions by whether they are in the process of being logged off or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LogonInProgress<Boolean>

Gets sessions by whether they are still executing user logon processing or not.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineName<String>

Gets sessions by their machine name (in the form DOMAIN\machine).

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineSummaryState<DesktopSummaryState>

Gets sessions on a machine with a specific summary state.

Valid values are Off, Unregistered, Available, Disconnected, Preparing, and InUse.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachineUid<Int32>

Gets sessions on a machine with the specified UID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-OSType<String>

Gets sessions with a specific type of operating system.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PersistUserChanges<PersistUserChanges>

Gets sessions where the user changes are persisted in a particular manner. Values can be:

o OnLocal - User changes are persisted locally.

o Discard - User changes are discarded.

o OnPvd - User changes are persisted on the Pvd.

Required?	false

Default Value	
Accept Pipeline Input?	false

-PowerState<PowerState>

Gets sessions on machines in the specified power state.

Valid values are Unmanaged, Unknown, Unavailable, On, Suspended, TurningOn, TurningOff, Suspending, and Resuming.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Protocol<String>

Get sessions by connection protocol. Valid values are HDX, RDP and Console.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningType<ProvisioningType>

Gets sessions hosted on machines provisioned in a particular manner. Values can be:

o Manual - No automated provisioning.

o PVS - Machine provisioned by PVS (machine may be physical, blade, VM,...).

o MCS - Machine provisioned by MCS (machine must be VM).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReceiverIPAddress<String>

Gets sessions with the specified client IP address supplied by Receiver (for example, StoreFront) when the session was launched, or reconnected.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReceiverName<String>

Gets sessions with the specified client name supplied by Receiver (for example, StoreFront) when the session was launched, or reconnected.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaActive<Boolean>

Get sessions by their use of SecureICA.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionId<Int32>

Deprecated.

Gets sessions by session ID, a unique identifier that Remote Desktop Services uses to track the session but it is only unique on that machine.

Required?	false
Default Value	

Accept Pipeline Input?	false

-SessionState<SessionState>

Get sessions by their state.

Valid values are Other, PreparingNewSession, Connected, Active, Disconnected, Reconnecting, NonBrokeredSession, and Unknown.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionStateChangeTime<DateTime>

Get sessions by their last state change time. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionSupport<SessionSupport>

Gets sessions hosted on machines which support the required pattern of sessions. Values can be:

o SingleSession - Single-session only machine.

o MultiSession - Multi-session capable machine.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionType<SessionType>

Get sessions by their type.

Valid values are Application and Desktop.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartTime<DateTime>

Get sessions by their start time. In general, Citrix recommends using -Filter and relative comparisons.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UntrustedUserName<String>

Gets sessions by the untrusted user name reported directly from the machine (in the form DOMAIN\user).

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserFullName<String>

Gets sessions by user's full name (usually 'first-name last-name').

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserName<String>

Get sessions by user name (in the form DOMAIN\user).

Required?	false

Default Value	
Accept Pipeline Input?	false

-UserSID<String>

Get sessions by user's Windows SID.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserUPN<String>

Gets sessions by user's User Principal Name (in the form user@domain).

Required?	false
Default Value	
Accept Pipeline Input?	false

-ApplicationUid<Int32>

Get sessions running the application with the specified Uid.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SharedDesktopUid<Int32>

Get sessions by SharedDesktop Uid.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Broker_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell style filter expression. See about_Broker_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.GroupInfo

Each GroupInfo object represents one group, and contains the following properties:

-- Count: The count of sessions in this group.

-- Name: The value of the property the sessions were grouped by (as a string).

If you do not specify -SortBy, groups are sorted with the largest count first.

Notes

To compare dates or times, use -Filter and relative comparisons. For more information, see about_Broker_Filtering and the

examples.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Group-BrokerSession -Property SessionState -DesktopGroupName dg1
```

Group sessions on machines from the dg1 group by session state.

---------- EXAMPLE 2 ----------

```
C:\PS> Group-BrokerSession -Property ClientName -ClientName 'ThinClient*' -SortBy Name
```

List alphabetically the names of the clients connected to the site, but only show clients whose names starts with 'ThinClient'.

Import-BrokerDesktopPolicy

Sep 10, 2014

Sets the site wide Citrix Group Policy settings for the site.

Syntax

```
Import-BrokerDesktopPolicy [-Policy] <Byte[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Import-BrokerDesktopPolicy sets the site wide Citrix Group Policy settings. A successful call to this cmdlet will result in the supplied data being uploaded to every machine in the site prior to its next session launch.

Related topics

Export-BrokerDesktopPolicy

New-BrokerConfigurationSlot

New-BrokerMachineConfiguration

Parameters

-Policy<Byte[]>

The configuration data containing the Citrix Group Policy settings to apply to every machine in the site.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.Byte[] The configuration data as an opaque binary blob.

Return Values

None

Notes

Import-BrokerDesktopPolicy performs a specialized operation. Direct usage of it in scripts is discouraged, and could result in data corruption. It is recommended that this operation be performed via the Citrix Studio.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Import-BrokerDesktopPolicy $policyData
```

This command sets the Citrix Group Policy settings in the site. These policy settings are then applied to every machine prior to the next session launch.

Move-BrokerAdminFolder

Sep 10, 2014

Moves a folder to another place in the hierarchy, optionally renaming it

Syntax

```
Move-BrokerAdminFolder [-InputObject] <AdminFolder[]> [-Destination] <AdminFolder> [-NewName <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Move-BrokerAdminFolder [-Name] <String> [-Destination] <AdminFolder> [-NewName <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Move-BrokerAdminFolder cmdlet moves a folder for organising objects for administration purposes (for example, Applications) to another position in the hierarchy.

The following special characters are not allowed in the new FolderName: \ / ; : # . * ? = < > | [ ] ( ) " ' `

Related topics

Get-BrokerAdminFolder

New-BrokerAdminFolder

Parameters

-InputObject<AdminFolder[]>

The folder(s) to be moved

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

A pattern matching the names of folders to be moved

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Destination<AdminFolder>

The destination folder the folder being moved should end up in

Required?	true
Default Value	
Accept Pipeline Input?	false

-NewName<String>

The name the new folder should have in the destination folder

Required?	false
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Depends on parameter Parameters can be piped by property name.

Return Values

None or Citrix.Broker.Admin.SDK.AdminFolder

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AdminFolder object.

Examples

---------- EXAMPLE 1 ----------

```
Move-BrokerAdminFolder F1\XXX\ F2\
```

Moves the folder called XXX within the folder F1\ to a new home in F2\

---------- EXAMPLE 2 ----------

```
Move-BrokerAdminFolder F1\XXX\ F2\ -NewName YYY
```

Moves the folder called XXX within the folder F1\ to a new home in F2\ renaming it to YYY in the process

Move-BrokerApplication

Sep 10, 2014

Move a published application from one admin folder to another

Syntax

```
Move-BrokerApplication [-InputObject] <Application[]> [-Destination] <AdminFolder> [-NewName <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Move-BrokerApplication [-Name] <String> [-Destination] <AdminFolder> [-NewName <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Move-BrokerApplication cmdlet moves a published application from one place to another in the tree of admin folders, optionally renaming it in the process (if you only want to change the name of the application for administrative purposes and not its location in the tree, use the Rename-BrokerApplication cmdlet).

The location and name of a published application in this sense is only of interest to the administrator, changes do not affect the end-user experience.

Related topics

New-BrokerApplication

Add-BrokerApplication

Get-BrokerApplication

Remove-BrokerApplication

Rename-BrokerApplication

Set-BrokerApplication

Parameters

-InputObject<Application[]>

The application(s) to be moved

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The application(s) to be moved

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Destination<AdminFolder>

The destination location within the admin folder hierarchy

Required?	true
Default Value	
Accept Pipeline Input?	false

-NewName<String>

The new name of the application in its new destination

Required?	false
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Application You can pipe applications to Move-BrokerApplication.

Return Values

None or Citrix.Broker.Admin.SDK.Application

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.Application object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Move-BrokerApplication -Name 'App1' -Destination 'F1\'
```

Moves the application in the root folder called "App1" to the folder "F1\".

---------- EXAMPLE 2 ----------

```
C:\PS> Move-BrokerApplication 'F1\App1' 'F2\' -NewName 'Application1'
```

Moves the application in folder "F1" called "App1" to the folder "F2\", renaming it to "Application1" in the process.

New-BrokerAccessPolicyRule

Sep 10, 2014

Creates a new rule in the site's access policy.

Syntax

New-BrokerAccessPolicyRule [-Name] <String> -DesktopGroupUid <Int32> [-AllowedConnections <AllowedConnection>] [-AllowedProtocols <String[]>] [-AllowedUsers <AllowedUser>] [-AllowRestart <Boolean>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedClientIPFilterEnabled <Boolean>] [-ExcludedClientIPs <IPAddressRange[]>] [-ExcludedClientNameFilterEnabled <Boolean>] [-ExcludedClientNames <String[]>] [-ExcludedSmartAccessFilterEnabled <Boolean>] [-ExcludedSmartAccessTags <String[]>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-HdxSslEnabled <Boolean>] [-IncludedClientIPFilterEnabled <Boolean>] [-IncludedClientIPs <IPAddressRange[]>] [-IncludedClientNameFilterEnabled <Boolean>] [-IncludedClientNames <String[]>] [-IncludedSmartAccessFilterEnabled <Boolean>] [-IncludedSmartAccessTags <String[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-BrokerAccessPolicyRule [-Name] <String> -IncludedDesktopGroups <DesktopGroup[]> [-IncludedDesktopGroupFilterEnabled <Boolean>] [-AllowedConnections <AllowedConnection>] [-AllowedProtocols <String[]>] [-AllowedUsers <AllowedUser>] [-AllowRestart <Boolean>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedClientIPFilterEnabled <Boolean>] [-ExcludedClientIPs <IPAddressRange[]>] [-ExcludedClientNameFilterEnabled <Boolean>] [-ExcludedClientNames <String[]>] [-ExcludedSmartAccessFilterEnabled <Boolean>] [-ExcludedSmartAccessTags <String[]>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-HdxSslEnabled <Boolean>] [-IncludedClientIPFilterEnabled <Boolean>] [-IncludedClientIPs <IPAddressRange[]>] [-IncludedClientNameFilterEnabled <Boolean>] [-IncludedClientNames <String[]>] [-IncludedSmartAccessFilterEnabled <Boolean>] [-IncludedSmartAccessTags <String[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The New-BrokerAccessPolicyRule cmdlet adds a new rule to the site's access policy.

An access policy rule defines a set of connection filters and access control rights relating to a desktop group. These allow fine-grained control of what access is granted to a desktop group based on details of, for example, a user's endpoint device, its address, and the user's identity.

Multiple rules in the access policy can apply to the same desktop group.

For a user to gain access to a desktop group via a rule their connection must match all its enabled include filters, and none of its enabled exclude filters. In addition, for a user to be able to launch a desktop or application resource session from the desktop group, they must have an entitlement to use the resource granted by the entitlement or assignment policies, or by direct machine assignment.

Related topics

Get-BrokerAccessPolicyRule

Set-BrokerAccessPolicyRule

Rename-BrokerAccessPolicyRule

Remove-BrokerAccessPolicyRule

Parameters

-Name<String>

Specifies the administrative name of the new rule. Each rule within the site's access policy must have a unique name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroupUid<Int32>

Specifies the desktop group to which the new rule applies.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IncludedDesktopGroups<DesktopGroup[]>

This parameter is supported for backward compatibility only. If used only a single desktop group UID can be specified.

The IncludedDesktopGroups and IncludedDesktopGroupFilterEnabled parameters have been superseded by the DesktopGroupUid parameter.

Required?	true
Default Value	(empty list)

Accept Pipeline Input?	true (ByPropertyName)

-AllowedConnections<AllowedConnection>

Specifies whether connections must be local or via Access Gateway, and if so whether specified SmartAccess tags must be provided by Access Gateway with the connection. This property forms part of the included SmartAccess tags filter.

Valid values are Filtered, NotViaAG, and ViaAG.

For a detailed description of this property see "help about_Broker_AccessPolicy".

Required?	false
Default Value	Filtered
Accept Pipeline Input?	true (ByPropertyName)

-AllowedProtocols<String[]>

Specifies the protocols (for example HDX, RDP) available to the user for sessions delivered from the new rule's desktop group. If the user gains access to a desktop group by multiple rules, the allowed protocol list is the combination of the protocol lists from all those rules.

If the protocol list is empty, access to the desktop group is implicitly denied.

Required?	false
Default Value	HDX
Accept Pipeline Input?	true (ByPropertyName)

-AllowedUsers<AllowedUser>

Specifies the behavior of the included users filter of the new rule. This can restrict access to a list of named users or groups, allow access to any authenticated user, any user (whether authenticated or not), or only non-authenticated users. For a detailed description of this property see "help about_Broker_AccessPolicy".

Valid values are Filtered, AnyAuthenticated, Any, AnonymousOnly and FilteredOrAnonymous.

Required?	false
Default Value	Filtered
Accept Pipeline Input?	true (ByPropertyName)

-AllowRestart<Boolean>

Specifies if the user can restart sessions delivered from the new rule's desktop group. Session restart is handled as follows: For sessions on single-session power-managed machines, the machine is powered off, and a new session launch request made; for sessions on multi-session machines, a logoff request is issued to the session, and a new session launch request made; otherwise the property is ignored.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Specifies an optional description of the new rule. The text is purely informational for the administrator, it is never visible to the end user.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Specifies whether the new rule is initially enabled. A disabled rule is ignored when evaluating the site's access policy.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedClientIPFilterEnabled<Boolean>

Specifies whether the excluded client IP address filter is initially enabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedClientIPs<IPAddressRange[]>

Specifies IP addresses of user devices explicitly denied access to the new rule's desktop group. Addresses can be specified as simple numeric addresses or as subnet masks (for example, 10.40.37.5 or 10.40.0.0/16). This property forms part of the excluded client IP address filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedClientNameFilterEnabled<Boolean>

Specifies whether the excluded client names filter is initially enabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedClientNames<String[]>

Specifies names of user devices explicitly denied access to the new rule's desktop group. This property forms part of the excluded client names filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedSmartAccessFilterEnabled<Boolean>

Specifies whether the excluded SmartAccess tags filter is initially enabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedSmartAccessTags<String[]>

Specifies SmartAccess tags which explicitly deny access to the new rule's desktop group if any occur in those provided by Access Gateway with the user's connection. This property forms part of the excluded SmartAccess tags filter.

Required?	false
Default Value	(empty list)

Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUserFilterEnabled<Boolean>

Specifies whether the excluded users filter is initially enabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUsers<User[]>

Specifies any users and groups who are explicitly denied access to the new rule's desktop group. This property forms part of the excluded users filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-HdxSslEnabled<Boolean>

Indicates whether SSL encryption is enabled for sessions delivered from the rule's desktop group.

Required?	false
Default Value	$false
Accept Pipeline Input?	true (ByPropertyName)

-IncludedClientIPFilterEnabled<Boolean>

Specifies whether the included client IP address filter is initially enabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-IncludedClientIPs<IPAddressRange[]>

Specifies IP addresses of user devices allowed access to the new rule's desktop group. Addresses can be specified as simple numeric addresses or as subnet masks (for example, 10.40.37.5 or 10.40.0.0/16). This property forms part of the included client IP address filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-IncludedClientNameFilterEnabled<Boolean>

Specifies whether the included client name filter is initially enabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-IncludedClientNames<String[]>

Specifies names of user devices allowed access to the new rule's desktop group. This property forms part of the included client names filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-IncludedSmartAccessFilterEnabled<Boolean>

Specifies whether the included SmartAccess tags filter is initially enabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-IncludedSmartAccessTags<String[]>

Specifies SmartAccess tags which grant access to the new rule's desktop group if any occur in those provided by Access Gateway with the user's connection. This property forms part of the excluded SmartAccess tags filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUserFilterEnabled<Boolean>

Specifies whether the included users filter is initially enabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUsers<User[]>

Specifies users and groups who are granted access to the new rule's desktop group. This property forms part of the included users filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

-IncludedDesktopGroupFilterEnabled<Boolean>

This parameter is supported for backward compatibility only. If used the supplied value must be $true.

The IncludedDesktopGroups and IncludedDesktopGroupFilterEnabled parameters have been superseded by the DesktopGroupUid parameter.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.AccessPolicyRule

New-BrokerAccessPolicyRule returns the newly created access policy rule.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Tech Support'
C:\PS> New-BrokerAccessPolicyRule 'UK Tech Support' -IncludedUserFilterEnabled $true -IncludedUsers support\uk-staff -DesktopGroupUid $dg.Uid -AllowedProtocols 'HDX
```

Creates an access policy rule allowing access to the Tech Support desktop group for all users of the SUPPORT\uk-staff group. Connections to desktop or application resources in the group can only be made using the HDX protocol.

For users to gain access to resources in the group also requires that, depending on the desktop kind of the group, appropriate assignment or entitlement policy rules, or explicit machine assignments exist.

New-BrokerAdminFolder

Sep 10, 2014

Creates a new admin folder.

Syntax

New-BrokerAdminFolder [-FolderName] <String> [-ParentFolder <AdminFolder>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The New-BrokerAdminFolder cmdlet creates a new folder for organising objects for administration purposes (for example, Applications).

New-BrokerAdminFolder creates the folder object and optionally places it within an existing admin folder if required.

The following special characters are not allowed in the FolderName: \ / ; : # . * ? = < > | [ ] ( ) " ' `

Related topics

Get-BrokerAdminFolder

Remove-BrokerAdminFolder

Parameters

-FolderName<String>

The simple name of the new folder within its parent (if any)

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ParentFolder<AdminFolder>

The name or UID of the parent folder (if any)

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Depends on parameter Parameters can be piped by property name.

Return Values

Citrix.Broker.Admin.SDK.AdminFolder

The new admin folder.

Examples

---------- EXAMPLE 1 ----------

```
New-BrokerAdminFolder F1
```

Creates an admin folder called F1 under the root folder (i.e. F1\)

---------- EXAMPLE 2 ----------

```
New-BrokerAdminFolder F2 -AdminFolder F1\
```

Creates an admin folder called F2 under the folder F1\ (i.e. F1\F2\)

New-BrokerAppAssignmentPolicyRule

Sep 10, 2014

Creates a new application rule in the site's assignment policy.

Syntax

```
New-BrokerAppAssignmentPolicyRule [-Name] <String> -DesktopGroupUid <Int32> [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The New-BrokerAppAssignmentPolicyRule cmdlet adds a new application rule to the site's assignment policy.

An application rule in the assignment policy defines the users who are entitled to a self-service persistent machine assignment from the rule's desktop group; once assigned the machine can run one or more applications published from the group.

The following constraints apply when creating an application assignment rule for a desktop group:

o The group's desktop kind must be Private

o The group's delivery type must be AppsOnly

o Only a single application rule can apply to a given group

o Application assignment rules cannot be applied to RemotePC groups.

When a user selects an application published from a private group, a currently unassigned machine is selected from the group and permanently assigned to the user. An application session is then launched to the machine. Subsequent launches are routed directly to the now assigned machine.

Once a machine has been assigned in this way, the original assignment rule plays no further part in access to the machine.

Related topics

Get-BrokerAppAssignmentPolicyRule

Set-BrokerAppAssignmentPolicyRule

Rename-BrokerAppAssignmentPolicyRule

Remove-BrokerAppAssignmentPolicyRule

Parameters

-Name<String>

Specifies the administrative name of the new application rule. Each rule in the site's assignment policy must have a unique name (irrespective of whether they are desktop or application rules).

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroupUid<Int32>

Specifies the unique ID of the desktop group to which the new application rule applies.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Specifies an optional description of the new application rule. The text is purely informational for the administrator, it is never visible to the end user.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Specifies whether the new application rule is initially enabled. A disabled rule is ignored when evaluating the site's assignment policy.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUserFilterEnabled<Boolean>

Specifies whether the excluded users filter is initially enabled. If the filter is disabled then any user entries in the filter are ignored when assignment policy rules are evaluated.

Required?	false
Default Value	false

Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUsers<User[]>

Specifies the excluded users filter of the new application rule, that is, the users and groups who are explicitly denied an entitlement to a machine assignment from the rule.

This can be used to exclude users or groups who would otherwise gain access by groups specified in the included users filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUserFilterEnabled<Boolean>

Specifies whether the included users filter is initially enabled. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to a machine assignment by the new application rule.

Users who would be implicitly granted access when the filter is disabled can still be explicitly denied access using the excluded users filter.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUsers<User[]>

Specifies the included users filter of the new application rule, that is, the users and groups who are granted an entitlement to a machine assignment by the rule.

If a user appears explicitly in the excluded users filter of the rule or is a member of a group that appears in the excluded users filter, no entitlement is granted whether or not the user appears in the included users filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director

typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.AppAssignmentPolicyRule

New-BrokerAppAssignmentPolicyRule returns the newly created application rule in the assignment policy.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Sales Support'
C:\PS> New-BrokerAppAssignmentPolicyRule 'UK Office' -DesktopGroupUid $dg.Uid -IncludedUsers sales\uk-staff
```

Creates an application rule in the assignment policy that grants all members of the SALES\uk-staff group an entitlement to a single machine from the Sales Support desktop group. The machine can be used for running applications published from the group.

New-BrokerAppEntitlementPolicyRule

Sep 10, 2014

Creates a new application rule in the site's entitlement policy.

Syntax

```
New-BrokerAppEntitlementPolicyRule [-Name] <String> -DesktopGroupUid <Int32> [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-SessionReconnection <SessionReconnection>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The New-BrokerAppEntitlementPolicyRule cmdlet adds a new application rule to the site's entitlement policy.

An application rule in the entitlement policy defines the users who are allowed per-session access to a machine to run one or more applications published from the rule's desktop group.

The following constraints apply when creating an application entitlement rule for a desktop group:

o The group's desktop kind must be Shared

o The group's delivery type must be AppsOnly or DesktopsAndApps

o Only a single application rule can apply to a given group

When a user selects an application published from a shared group, a machine is selected from the group on which to run the application. No permanent association exists between the user and the selected machine; once the session ends the association also ends.

Even though only a single application entitlement and therefore session can be defined for a group, the user can still run multiple applications from the group because the applications run within the same session.

Related topics

Get-BrokerAppEntitlementPolicyRule

Set-BrokerAppEntitlementPolicyRule

Rename-BrokerAppEntitlementPolicyRule

Remove-BrokerAppEntitlementPolicyRule

Parameters

-Name<String>

Specifies the administrative name of the new application rule. Each rule in the site's entitlement policy must have a unique name (irrespective of whether they are desktop or application rules).

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroupUid<Int32>

Specifies the unique ID of the desktop group to which the new application rule applies.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Specifies an optional description of the new application rule. The text is purely informational for the administrator, it is never visible to the end user.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Specifies whether the new application rule is initially enabled. A disabled rule is ignored when evaluating the site's entitlement policy.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUserFilterEnabled<Boolean>

Specifies whether the excluded users filter is initially enabled. If the filter is disabled then any user entries in the filter are ignored when entitlement policy rules are evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUsers<User[]>

Specifies the excluded users filter of the application rule, that is, the users and groups who are explicitly denied entitlements to published applications from the desktop group.

This can be used to exclude users or groups who would otherwise gain access by groups specified in the included users filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUserFilterEnabled<Boolean>

Specifies whether the included users filter is initially enabled. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to an application session by the new rule.

Users who would be implicitly granted access when the filter is disabled can still be explicitly denied access using the excluded users filter.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUsers<User[]>

Specifies the included users filter of the application rule, that is, the users and groups who are granted an entitlement to an application session by the new rule.

If a user appears explicitly in the excluded users filter of the rule or is a member of a group that appears in the excluded users filter, no entitlement is granted whether or not the user appears in the included users filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-SessionReconnection<SessionReconnection>

Defines reconnection (roaming) behavior for sessions launched using this rule. Session reconnection control is an experimental and unsupported feature.

Required?	false
Default Value	Always

Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.AppEntitlementPolicyRule

New-BrokerAppEntitlementPolicyRule returns the newly created application rule in the entitlement policy.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Customer Support'
C:\PS> New-BrokerAppEntitlementPolicyRule 'UK Office' -DesktopGroupUid $dg.Uid -IncludedUsers support\uk-staff
```

Creates an application rule in the entitlement policy that entitles all members of the SUPPORT\uk-staff group to a machine for running applications published from the Customer Support desktop group.

New-BrokerApplication

Sep 10, 2014

Creates a new published application.

Syntax

New-BrokerApplication [-Name] <String> -CommandLineExecutable <String> -DesktopGroup <DesktopGroup> [-AdminFolder <AdminFolder>] [-ApplicationType <ApplicationType>] [-BrowserName <String>] [-ClientFolder <String>] [-CommandLineArguments <String>] [-CpuPriorityLevel <CpuPriorityLevel>] [-Description <String>] [-Enabled <Boolean>] [-IconFromClient <Boolean>] [-IconUid <Int32>] [-Priority <Int32>] [-PublishedName <String>] [-SecureCmdLineArgumentsEnabled <Boolean>] [-ShortcutAddedToDesktop <Boolean>] [-ShortcutAddedToStartMenu <Boolean>] [-StartMenuFolder <String>] [-UserFilterEnabled <Boolean>] [-UUID <Guid>] [-Visible <Boolean>] [-WaitForPrinterCreation <Boolean>] [-WorkingDirectory <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The New-BrokerApplication cmdlet creates a new published application in the site.

New-BrokerApplication creates the application object, and associates it with a desktop group. Application objects have three names that identify them (in addition to their Uid): the Name, BrowserName and the PublishedName. The BrowserName is unique across the entire site, and is primarily used internally. The Name is also unique and is what is seen by the administrator; it contains any prefix for an enclosing admin folder (if any). The PublishedName is not unique and is what is seen by the users.

You can create both HostedOnDesktop and InstalledOnClient applications but the ApplicationType cannot be changed later.

The following special characters are not allowed in the Name, BrowserName or the PublishedName properties: \ / ; : # . * ? = < > | [ ] ( ) " '

In addition the ` character is not allowed in the Name property.

See about_Broker_Applications for more information.

Related topics

Add-BrokerApplication

Remove-BrokerApplication

Get-BrokerApplication

Remove-BrokerApplication

Rename-BrokerApplication

Move-BrokerApplication

Set-BrokerApplication

Parameters

-Name<String>

Specifies the name of the application (must be unique within folder).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-CommandLineExecutable<String>

Specifies the name of the executable file to launch. The full path need not be provided if it's already in the path. Environment variables can also be used.

Required?	true
Default Value	(required)
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroup<DesktopGroup>

Specifies which desktop group this application should be associated with. The association between application and desktop groups can be added or removed using the Add-

BrokerApplication and Remove-BrokerApplication cmdlets.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-AdminFolder<AdminFolder>

The folder in which the new application should reside (if any).

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ApplicationType<ApplicationType>

Specifies the type of the application: HostedOnDesktop or InstalledOnClient.

Required?	false
Default Value	(required)
Accept Pipeline Input?	true (ByPropertyName)

-BrowserName<String>

Specifies the internal name for this application. It must be unique in the site.

Required?	false
Default Value	(same as Name)
Accept Pipeline Input?	true (ByPropertyName)

-ClientFolder<String>

Specifies the folder that the application belongs to as the user sees it. This is the application folder that is seen in the Citrix Online Plug-in, in Web Services, and also in the end-user's Start menu. Subdirectories can be specified with '\' character. The following special characters are not allowed: / * ? < > | " :. Note that this property cannot be set for applications of type InstalledOnClient.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-CommandLineArguments<String>

Specifies the command-line arguments to use when launching the executable. Environment variables can be used.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-CpuPriorityLevel<CpuPriorityLevel>

Specifies the CPU priority for the launched process. Valid values are: Low, BelowNormal, Normal, AboveNormal, and High. Note that this property cannot be set for applications of type InstalledOnClient.

Required?	false
Default Value	Normal
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Specifies the description of the application. This is only seen by Citrix administrators and is not visible to users.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Specifies whether or not this application can be launched.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-IconFromClient<Boolean>

Specifies if the app icon should be retrieved from the application on the client. This is reserved for possible future use, and all applications of type HostedOnDesktop cannot set or change this value.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-IconUid<Int32>

Specifies which icon to use for this application. This icon is visible both to the administrator (in the consoles) and to the user. If no icon is specified, then a generic built-in application icon is used.

Required?	false
Default Value	2
Accept Pipeline Input?	true (ByPropertyName)

-Priority<Int32>

Specifies the priority of the mapping between the application and desktop group. A value of zero has the highest priority, with increasing values indicating lower priorities.

Required?	false
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-PublishedName<String>

The name seen by end users who have access to this application.

Required?	false
Default Value	The same value as that supplied for the name of the application.
Accept Pipeline Input?	true (ByPropertyName)

-SecureCmdLineArgumentsEnabled<Boolean>

Specifies whether the command-line arguments are secured or not. This is reserved for possible future use, and all applications of type HostedOnDesktop can only have this value set to true.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-ShortcutAddedToDesktop<Boolean>

Specifies whether or not a shortcut to the application should be placed on the user device. This is valid only for the Citrix Online Plug-in.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-ShortcutAddedToStartMenu<Boolean>

Specifies whether a shortcut to the application should be placed in the user's start menu on their user device.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-StartMenuFolder<String>

Specifies the name of the start menu folder that holds the application shortcut (if any). This is valid only for the Citrix Online Plug-in. Subdirectories can be specified with '\' character. The following special characters are not allowed: / * ? < > | " :.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-UserFilterEnabled<Boolean>

Specifies whether the application's user filter is enabled or disabled. Where the user filter is enabled, the application is visible only to users who appear in the filter (either explicitly or by virtue of group membership).

Required?	false

Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-UUID<Guid>

An optional GUID for this application.

Required?	false
Default Value	A new GUID is generated if none is supplied.
Accept Pipeline Input?	true (ByPropertyName)

-Visible<Boolean>

Specifies whether or not this application is visible to users. Note that it's possible for an application to be disabled and still visible.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-WaitForPrinterCreation<Boolean>

Specifies whether or not the session waits for the printers to be created before allowing the user to interact with the session. Note that this property cannot be set for applications of type InstalledOnClient.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-WorkingDirectory<String>

Specifies which working directory the executable is launched from. Environment variables can be used.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Depends on parameter Parameters can be piped by property name.

Return Values

Citrix.Broker.Admin.SDK.Application

New-BrokerApplication returns an Application object.

Notes

Usually only the Name is specified with the New-BrokerApplication cmdlet, and the system chooses a BrowserName and PublishedName for you. By default the BrowserName is the same as the Name, if it is unique in the site. If not, then "-x" is appended to the name, where "x" is a number. For instance, if there is already an application with a BrowserName of "Notepad" and a new application is created with a Name of "Notepad", then the new application gets a BrowserName of "Notepad-1". If another "Notepad" is published, it has a BrowserName of "Notepad-2".

That said, the BrowserName can optionally be specified as well.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-BrokerApplication -ApplicationType HostedOnDesktop -Name "Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup PrivateDG1
```

Creates and returns an object for a published application called "Notepad" that launches "notepad.exe".

---------- EXAMPLE 2 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup "SharedDG1"
C:\PS> $app = New-BrokerApplication -ApplicationType HostedOnDesktop -Name "Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg
C:\PS> $group = Get-BrokerDesktopGroup -Name "Shared desktop group"
C:\PS> Add-BrokerApplication $app -DesktopGroup $group
C:\PS> $fta = Get-BrokerImportedFTA -ExtensionName ".txt"
C:\PS> New-BrokerConfiguredFTA -ImportedFTA $fta -ApplicationUid $app.Uid
```

This is a much more complete example. It creates an application object to publish Notepad and associates it first with the "SharedDG1" desktop group.

Next it adds an additional desktop group (one that can host applications), and publishes the application to that desktop group. It then gets the ImportedFTA object for the .txt file-type extension (this assumes file-type associations have already been imported), and then configures it so that ".txt" is associated with the published application.

Note: The appropriate access policy and app assignment/entitlement rules must also be configured to allow access to the application.

New-BrokerAssignmentPolicyRule

Sep 10, 2014

Creates a new desktop rule in the site's assignment policy.

Syntax

New-BrokerAssignmentPolicyRule [-Name] <String> -DesktopGroupUid <Int32> [-ColorDepth <ColorDepth>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IconUid <Int32>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-MaxDesktops <Int32>] [-PublishedName <String>] [-SecureIcaRequired <Boolean>] [-UUID <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The New-BrokerAssignmentPolicyRule cmdlet adds a new desktop rule to the site's assignment policy.

A desktop rule in the assignment policy defines the users who are entitled to self-service persistent machine assignments from the rule's desktop group. A rule defines how many machines a user is allowed from the group for delivery of full desktop sessions.

The following constraints apply when creating a desktop assignment rule for a desktop group:

o The group's desktop kind must be Private

o The group's delivery type must be DesktopsOnly

o Only one desktop assignment rule can be created for RemotePC groups.

When a user selects a machine assignment entitlement from a private group, a currently unassigned machine is selected from the group and permanently assigned to the user to create an assigned desktop. A desktop session is then launched to the machine. Subsequent launches are routed directly to the now assigned machine.

Once a machine has been assigned in this way, the original assignment rule plays no further part in access to the new desktop.

Multiple desktop rules in the assignment policy can apply to the same desktop group. Where a user is granted entitlements by more than one rule for the same group, they can have as many machine assignments from the group as the total of their entitlements.

Related topics

Get-BrokerAssignmentPolicyRule

Set-BrokerAssignmentPolicyRule

Rename-BrokerAssignmentPolicyRule

Remove-BrokerAssignmentPolicyRule

Parameters

-Name<String>

Specifies the administrative name of the new desktop rule. Each rule in the site's assignment policy must have a unique name (irrespective of whether they are desktop or application rules).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroupUid<Int32>

Specifies the unique ID of the desktop group to which the new desktop rule applies.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-ColorDepth<ColorDepth>

Specifies the color depth of any desktop sessions to machines assigned by the new rule.

Valid values are $null, FourBit, EightBit, SixteenBit, and TwentyFourBit.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Specifies an optional description of the new desktop rule. The text may be visible to the end user, for example, as a tooltip associated with the desktop entitlement.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Specifies whether the new desktop rule is initially enabled. A disabled rule is ignored when evaluating the site's assignment policy.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUserFilterEnabled<Boolean>

Specifies whether the excluded users filter is initially enabled. If the filter is disabled then any user entries in the filter are ignored when assignment policy rules are evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUsers<User[]>

Specifies the excluded users filter of the new desktop rule, that is, the users and groups who are explicitly denied an entitlement to a machine assignment from the rule.

This can be used to exclude users or groups who would otherwise gain access by groups specified in the included users filter.

Required?	false

Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-IconUid<Int32>

Specifies the unique ID of the icon used to display the machine assignment entitlement to the user, and of the assigned desktop itself following the assignment.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUserFilterEnabled<Boolean>

Specifies whether the included users filter is initially enabled. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to a machine assignment by the new desktop rule.

Users who would be implicitly granted access when the filter is disabled can still be explicitly denied access using the excluded users filter.

For rules that relate to RemotePC desktop groups however, if the included user filter is disabled, the rule is effectively disabled.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUsers<User[]>

Specifies the included users filter of the new desktop rule, that is, the users and groups who are granted an entitlement to a machine assignment by the rule.

If a user appears explicitly in the excluded users filter of the rule or is a member of a group that appears in the excluded users filter, no entitlement is granted whether or not the user appears in the included users filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-MaxDesktops<Int32>

The number of machines from the rule's desktop group to which a user is entitled. Where an entitlement is granted to a user group rather than an individual, the number of machines applies to each member of the user group independently.

Required?	false
Default Value	1
Accept Pipeline Input?	true (ByPropertyName)

-PublishedName<String>

The name of the new machine assignment entitlement as seen by the user, and of the assigned desktop following its usage.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-SecureIcaRequired<Boolean>

Specifies whether the new desktop rule requires the SecureICA protocol to be used for desktop sessions to machines assigned using the entitlement.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-UUID<Guid>

An optional GUID for this rule.

Required?	false
Default Value	A new GUID is generated if none is supplied.
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.AssignmentPolicyRule

New-BrokerAssignmentPolicyRule returns the newly created desktop rule in the assignment policy rule.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Sales Support'
C:\PS> New-BrokerAssignmentPolicyRule 'UK Office' -DesktopGroupUid $dg.Uid -IncludedUsers sales\uk-staff -PublishedName 'Sales Desktop'
```

Creates a desktop rule in the assignment policy that grants all members of the SALES\uk-staff group an entitlement to a single machine from the Sales Support desktop group. The entitlement name seen by users is Sales Desktop.

New-BrokerCatalog

Sep 10, 2014

Adds a new catalog to the site.

Syntax

New-BrokerCatalog [-Name] <String> [-AllocationType] <AllocationType> [-CatalogKind] <CatalogKind> [-PvsForVM <String[]>] [-Description <String>] [-IsRemotePC <Boolean>] [-MachinesArePhysical <Boolean>] [-MinimumFunctionalLevel <FunctionalLevel>] [-PvsAddress <String>] [-PvsDomain <String>] [-RemotePCHypervisorConnectionUid <Int32>] [-Scope <String[]>] [-UUID <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-BrokerCatalog [-Name] <String> [-AllocationType] <AllocationType> [-ProvisioningType] <ProvisioningType> [-SessionSupport] <SessionSupport> [-PersistUserChanges] <PersistUserChanges> [-ProvisioningSchemeId <Guid>] [-Description <String>] [-IsRemotePC <Boolean>] [-MachinesArePhysical <Boolean>] [-MinimumFunctionalLevel <FunctionalLevel>] [-PvsAddress <String>] [-PvsDomain <String>] [-RemotePCHypervisorConnectionUid <Int32>] [-Scope <String[]>] [-UUID <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

New-BrokerCatalog adds a catalog through which machines can be provided to the site.

In order for a machine to register in a site, the machine must belong to a catalog with which it is compatible. The compatibility of a machine with a catalog is determined by two of the parameters of New-BrokerCatalog:

o MinimalFunctionalLevel: The minimal functional level supported in the catalog. The functional level of the machine is determined by the capabilities of the Citrix VDA software on it.

o SessionSupport: The session support (single/multi) of the catalog. The session support of the machine is determined by the variant of the Citrix VDA software installed (workstation/terminal services, respectively).

Related topics

Get-BrokerCatalog

Rename-BrokerCatalog

Remove-BrokerCatalog

Set-BrokerCatalog

Parameters

-Name<String>

Specifies a name for the catalog. Each catalog within a site must have a unique name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-AllocationType<AllocationType>

Specifies how machines in the catalog are assigned to users. Values can be:

o Static - Machines in a catalog of this type are permanently assigned to a user.

o Permanent - equivalent to 'Static'.

o Random - Machines in a catalog of this type are picked at random and temporarily assigned to a user.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-CatalogKind<CatalogKind>

Deprecated: The type of machines the catalog will contain. Values can be: ThinCloned, SingleImage, PowerManaged, Unmanaged, Pvs, Pvd or PvsPvd.

Thin-Cloned, Single-Image and Personal vDisk Catalogs

Thin-cloned and single-image catalog kinds are for machines created and managed with Provisioning Services for VMs. All machines in this type of catalog are managed, and so must be associated with a hypervisor connection.

A thin-cloned catalog is used for original golden VM images that are cloned when they are assigned to a VM, and users' changes to the VM image are retained after the VM is restarted.

A single-image catalog is used when multiple machines provisioned with Provisioning Services for VMs all share a single golden VM image when they run and, when restarted, they revert to the original

VM image state.

A personal vDisk catalog is similar to a single-image catalog, but it also uses personal vDisk technology.

PowerManaged

This catalog kind is for managed machines that are manually provisioned by administrators. All machines in this type of catalog are managed, and so must be associated with a hypervisor connection.

Unmanaged

This catalog kind is for unmanaged machines, so there is no associated hypervisor connection.

PVS

This catalog kind is for managed machines that are provisioned using Provisioning Services. All machines in this type of catalog are managed, and so must be associated with a hypervisor connection. Only shared desktops are suitable for this catalog kind.

A Provisioning Services-personal vDisk (PvsPvd) catalog is similar to a Provisioning Services catalog, but it also uses personal vDisk technology.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningType<ProvisioningType>

Specifies the ProvisioningType for the catalog. Values can be:

o Manual - No provisioning.

o PVS - Machine provisioned by PVS (machine may be physical, blade, VM,...).

o MCS - Machine provisioned by MCS (machine must be VM).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-SessionSupport<SessionSupport>

Specifies whether machines in the catalog are single or multi-session capable. Values can be:

o SingleSession - Single-session only machine.

o MultiSession - Multi-session capable machine.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PersistUserChanges<PersistUserChanges>

Specifies how user changes are persisted on machines in the catalog. Possible values are:

o OnLocal: User changes are stored on the machine's local storage.

o Discard: User changes are discarded.

o OnPvd: User changes are stored on the user's personal vDisk.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PvsForVM<String[]>

Deprecated:

Identifies the provisioning scheme used by this catalog. To be specified in the format: ProvisioningSchemeGuid:ServiceGroupGuid. Applicable only to thin-cloned, single-image or personal vDisk catalogs.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

A description for the catalog.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IsRemotePC<Boolean>

Specifies whether this is to be a Remote PC catalog.

IsRemotePC can only be enabled when:

o SessionSupport is SingleSession

o MachinesArePhysical is true.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-MachinesArePhysical<Boolean>

Specifies whether machines in the catalog can be power-managed by the Citrix Broker Service. Where the Citrix Broker Service cannot control the power state of themachine specify $true, otherwise $false. Can only be specified together with a provisioning type of Pvs or Manual, or if used with the legacy CatalogKind parameter only with Pvs or PvsPvd catalog kinds.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-MinimumFunctionalLevel<FunctionalLevel>

The minimum FunctionalLevel required for machines to register in the site.

Valid values are L5, L7, L7_6

Required?	false
Default Value	The FunctionalLevel of the current release (L7_6); by default no machines with less than the most current FunctionalLevel will be functional.
Accept Pipeline Input?	true (ByPropertyName)

-PvsAddress<String>

Specifies the URL of the Provisioning Services server. Only applicable to Provisioning Services or Provisioning Services-personal vDisk catalogs.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PvsDomain<String>

Specifies the Active Directory domain of the Provisioning Services server. Only applicable to Provisioning Services or Provisioning Services-personal vDisk catalogs.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-RemotePCHypervisorConnectionUid<Int32>

Specifies the hypervisor connection to use for powering on remote PCs in this catalog (only allowed when IsRemotePC is true).

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Scope<String[]>

Specifies the name of the delegated administration scope to which the catalog belongs.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-UUID<Guid>

An optional GUID for this catalog.

Required?	false
Default Value	A new GUID is generated if none is supplied.
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

-ProvisioningSchemeId<Guid>

Specifies the identity of the MCS provisioning scheme the new catalog is associated with (can only be specified for new catalogs with a ProvisioningType of MCS).

Required?	false

Default Value	$null
Accept Pipeline Input?	true (ByPropertyName)

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Catalog

New-BrokerCatalog returns the created catalog.

Examples

---------- EXAMPLE 1 ----------

C:\PS> New-BrokerCatalog -AllocationType Static -CatalogKind Unmanaged -Description "Catalog1 Description" -Name "Catalog1 Name"
This command creates a catalog that can contain unmanaged physical or virtual machines that are permanently assigned to the user.

---------- EXAMPLE 2 ----------

C:\PS> New-BrokerCatalog -AllocationType Random -CatalogKind PowerManaged -Description "catalog 2 Description" -Name "Catalog2 Name"
This command creates a catalog that can contain power-managed machines that are randomly assigned to the user.

---------- EXAMPLE 3 ----------

C:\PS> New-BrokerCatalog -AllocationType Random -CatalogKind PVS -Description "PVS Catalog Desc" -Name "PVS Catalog Name" -PvsAddress "pvsServer@pvsDomain.cor
This command creates a catalog that can contain managed machines that are provisioned using Provisioning Services.

New-BrokerConfigurationSlot

Sep 10, 2014

Creates a new configuration slot.

Syntax

New-BrokerConfigurationSlot [-Name] <String> -SettingsGroup <String> [-Description <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Creates a new configuration slot. The SettingsGroup of the slot determines the particular collection of related settings that may be specified in a machine configuration associated with this slot.

For example, the configuration slot may be restricted to configuring Citrix User Profile Manager settings by specifying the SettingsGroup parameter as "G=UPM".

Related topics

Get-BrokerConfigurationSlot

Remove-BrokerConfigurationSlot

New-BrokerMachineConfiguration

Parameters

-Name<String>

Name of the new configuration slot. This must be alphanumeric and not contain white space.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-SettingsGroup<String>

The settings group determines the particular collection of related settings that may be controlled by this slot. This must match the format of a Citrix Group Policy configuration group (e.g. "G=UPM"). Only settings that have this exact group may be specified in a machine configuration associated with this configuration slot.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Description of configuration slot.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.ConfigurationSlot

New-BrokerConfigurationSlot returns an object representing the newly created configuration slot

Examples

---------- EXAMPLE 1 ----------

```
New-BrokerConfigurationSlot -Name "UPM" -SettingsGroup "G=UPM"
```

Create a new slot named "UPM" to configure settings specific to "User Profile Management"

New-BrokerConfiguredFTA

Sep 10, 2014

Creates a file type association with a published application.

Syntax

New-BrokerConfiguredFTA -ImportedFTA <ImportedFTA> -ApplicationUid <Int32> [-UUID <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-BrokerConfiguredFTA -ExtensionName <String> -HandlerName <String> -ApplicationUid <Int32> [-ContentType <String>] [-HandlerDescription <String>] [-HandlerOpenArguments <String>] [-UUID <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Creates an association between a file type and a published application for the purposes of the content redirection.

File type association associates a file extension (such as ".txt") with an application (such as Notepad). In a Citrix environment file type associations on a user device can be configured so that when an user clicks on a document it launches the appropriate published application. This is known as "content redirection".

Configured file type associations are different from imported file type associations. Configured file type associations are those that are actually associated with published applications for the purposes of content redirection. Imported file type associations are lists of known file type associations for a given desktop group. See Update-BrokerImportedFTA for more information about imported file type associations.

This cmdlet has two parameter sets, which correspond to the cmdlet's two use cases.

The first use case leverages imported file type associations to configure file types for published applications. Information about the file type association is read from the imported object. See the Update-BrokerImportedFTA cmdlet for more information about importing file type associations from a worker machine.

The second use case is more complex and allows you to create your own file type association without having to import it first. This also lets you create custom file type associations that may not already exist on the worker machines. This use case is more error-prone, however, because the individual attributes of the file type association must be correctly specified by you.

Related topics

Get-BrokerImportedFTA

Get-BrokerConfiguredFTA

Remove-BrokerConfiguredFTA

Parameters

-ApplicationUid<Int32>

Specifies the application with which the file type should be associated.

Required?	true
Default Value	(required)
Accept Pipeline Input?	true (ByPropertyName)

-ImportedFTA<ImportedFTA>

Specifies the ImportedFTA object to use for creating the ConfiguredFTA object. All values needed to create a ConfiguredFTA object are read from the ImportedFTA object.

Required?	true
Default Value	(required)
Accept Pipeline Input?	true (ByPropertyName)

-ExtensionName<String>

Specifies the extension name for the file type association. For example, ".txt" or ".doc".

Required?	true
Default Value	(required)
Accept Pipeline Input?	true (ByPropertyName)

-HandlerName<String>

Specifies the name of the handler for the file type association (as seen in the Registry). For example, "TXTFILE" or "Word.Document.8".

Required?	true

Default Value	(required)
Accept Pipeline Input?	true (ByPropertyName)

-UUID<Guid>

An optional GUID for this ConfiguredFTA.

Required?	false
Default Value	A new GUID is generated if none is supplied.
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

-ContentType<String>

Specifies the content type of the file type (as listed in the Registry). For example, content type would be "text/plain" or "application/msword".

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-HandlerDescription<String>

Specifies the description of the handler for the file type association.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-HandlerOpenArguments<String>

Specifies the arguments for the open command that the handler should use. For example, "%1".

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

Input Type

Variable, based on property name. This cmdlet does accept input from the pipeline but only by property name.

Return Values

Citrix.Broker.Admin.SDK.ConfiguredFTA

This cmdlet returns a single ConfiguredFTA object.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS> $app = Get-BrokerApplication "Notepad"
C:\PS> $fta = Get-BrokerImportedFTA -ExtensionName ".txt"
C:\PS> New-BrokerConfiguredFTA -ImportedFTA $fta -ApplicationUid $app.Uid
```

Gets the Uid for the application, gets the ImportedFTA object for the file extension, and finally associates ".txt" with the published "Notepad" application.

Note that the Get-BrokerImportedFTA cmdlet may return more than one ImportedFTA objects for a specific extension name. See the help for that cmdlet for more details.

-------------------------- EXAMPLE 2 --------------------------

```
C:\PS> $app = Get-BrokerApplication "Notepad"
C:\PS> New-BrokerConfiguredFTA -ApplicationUid $app.Uid -ExtensionName ".txt" -HandlerName "txtfile" -ContentType "text\plain" -HandlerDescription "Text Document" -
```

This example is identical to the first, but shows the the second use case of the cmdlet, specifying each attribute manually.

New-BrokerDelayedHostingPowerAction

Sep 10, 2014

Causes a power action to be queued after a delay.

Syntax

```
New-BrokerDelayedHostingPowerAction [-MachineName] <String> -Action <PowerManagementAction> -Delay <TimeSpan> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Causes a power action to be queued after the specified period of time.

Only ShutDown or Suspend actions can be requested to be delayed in this manner.

For a detailed description of the queuing mechanism, see 'help about_Broker_PowerManagement'.

Related topics

Get-BrokerDelayedHostingPowerAction

New-BrokerDelayedHostingPowerAction

Parameters

-MachineName<String>

Specifies the machine that the action is to be performed on.

The machine can be identified by DNS name, short name, SID, or name of the form domain\machine.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Action<PowerManagementAction>

Specifies the power state change action that is to be performed on the specified machine after the specified delay.

Valid values are Shutdown and Suspend.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Delay<TimeSpan>

Specifies a timespan delay before the action is queued.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.DelayedHostingPowerAction

New-BrokerDelayedHostingPowerAction returns the created delayed power action.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-BrokerDelayedHostingPowerAction -Action Shutdown -MachineName 'XD_VDA1' -Delay '00:02:00'
```

Causes the machine called XD_VDA1 to be shut down after a delay of two minutes.

New-BrokerDesktopGroup

Sep 10, 2014

Create a new desktop group for managing the brokering of groups of desktops.

Syntax

New-BrokerDesktopGroup [-Name] <String> -DesktopKind <DesktopKind> [-AutomaticPowerOnForAssigned <Boolean>] [-AutomaticPowerOnForAssignedDuringPeak <Boolean>] [-ColorDepth <ColorDepth>] [-DeliveryType <DeliveryType>] [-Description <String>] [-Enabled <Boolean>] [-IconUid <Int32>] [-InMaintenanceMode <Boolean>] [-IsRemotePC <Boolean>] [-MinimumFunctionalLevel <FunctionalLevel>] [-OffPeakBufferSizePercent <Int32>] [-OffPeakDisconnectAction <SessionChangeHostingAction>] [-OffPeakDisconnectTimeout <Int32>] [-OffPeakExtendedDisconnectAction <SessionChangeHostingAction>] [-OffPeakExtendedDisconnectTimeout <Int32>] [-OffPeakLogOffAction <SessionChangeHostingAction>] [-OffPeakLogOffTimeout <Int32>] [-PeakBufferSizePercent <Int32>] [-PeakDisconnectAction <SessionChangeHostingAction>] [-PeakDisconnectTimeout <Int32>] [-PeakExtendedDisconnectAction <SessionChangeHostingAction>] [-PeakExtendedDisconnectTimeout <Int32>] [-PeakLogOffAction <SessionChangeHostingAction>] [-PeakLogOffTimeout <Int32>] [-ProtocolPriority <String[]>] [-PublishedName <String>] [-Scope <String[]>] [-SecureIcaRequired <Boolean>] [-SessionSupport <SessionSupport>] [-SettlementPeriodBeforeAutoShutdown <TimeSpan>] [-ShutdownDesktopsAfterUse <Boolean>] [-TimeZone <String>] [-TurnOnAddedMachine <Boolean>] [-UUID <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The New-BrokerDesktopGroup cmdlet creates a new broker desktop group that can then be used to manage the brokering settings of all desktops within that desktop group. Once the desktop group has been created, you can create desktops in it by adding the appropriate broker machines to it using the Add-BrokerMachine or Add-BrokerMachinesToDesktopGroup cmdlets.

Desktop groups hold settings that apply to all desktops they contain.

For any automatic power management settings of a desktop group to take effect, the group's TimeZone property must be specified. Automatic power management operations include pool management (power time schemes), reboot schedules, session disconnect and logoff actions, and powering on assigned machines etc.

Related topics

Get-BrokerDesktopGroup

Set-BrokerDesktopGroup

Rename-BrokerDesktopGroup

Remove-BrokerDesktopGroup

Add-BrokerMachine

Add-BrokerMachinesToDesktopGroup

Get-BrokerSite

Parameters

-Name<String>

The name of the new broker desktop group.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopKind<DesktopKind>

The kind of desktops this group will hold. Valid values are Private and Shared.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-AutomaticPowerOnForAssigned<Boolean>

Specifies whether assigned desktops in the desktop group should be automatically started at the start of peak time periods. Only relevant for groups whose DesktopKind is Private.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-AutomaticPowerOnForAssignedDuringPeak<Boolean>

Specifies whether assigned desktops in the desktop group should be automatically started throughout peak time periods. Only relevant for groups whose DesktopKind is Private and which have AutomaticPowerOnForAssigned set to true.

Required?	false
Default Value	false

Accept Pipeline Input?	true (ByPropertyName)

-ColorDepth<ColorDepth>

Specifies the color depth that the ICA session should use for desktops in this group. Valid values are FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	TwentyFourBit
Accept Pipeline Input?	true (ByPropertyName)

-DeliveryType<DeliveryType>

Specifies whether desktops, applications, or both, can be delivered from machines contained within the new desktop group. Desktop groups with a DesktopKind of Private cannot be used to deliver both desktops and applications. Defaults to DesktopsOnly if not specified.

Valid values are DesktopsOnly, AppsOnly, and DesktopsAndApps.

Required?	false
Default Value	DesktopsOnly
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

A description for this desktop group useful for administrators of the site.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Whether the desktop group should be in the enabled state; disabled desktop groups do not appear to users.

Required?	false

Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-IconUid<Int32>

The UID of the broker icon to be displayed to users for their desktop(s) in this desktop group.

Required?	false
Default Value	The Uid of the default desktop icon in this site - use the Get-BrokerSite cmdlet to find this value.
Accept Pipeline Input?	true (ByPropertyName)

-InMaintenanceMode<Boolean>

Whether the desktop should be created in maintenance mode; a desktop group in maintenance mode will not allow users to connect or reconnect to their desktops.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-IsRemotePC<Boolean>

Specifies whether this is to be a Remote PC desktop group.

IsRemotePC can only be enabled when:

o SessionSupport is SingleSession

o DeliveryType is DesktopsOnly

o DesktopKind is Private

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-MinimumFunctionalLevel<FunctionalLevel>

The minimum FunctionalLevel required for machines to work successfully in the desktop group.

Valid values are L5, L7, L7_6

Required?	false
Default Value	The FunctionalLevel of the current release (L7_6); by default no machines with less than the most current FunctionalLevel will be functional.
Accept Pipeline Input?	true (ByPropertyName)

-OffPeakBufferSizePercent<Int32>

The percentage of machines in the desktop group that should be kept available in an idle state outside peak hours.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-OffPeakDisconnectAction<SessionChangeHostingAction>

The action to be performed after a configurable period of a user session disconnecting outside peak hours. Possible values are Nothing, Suspend, or Shutdown

Required?	false
Default Value	Nothing
Accept Pipeline Input?	true (ByPropertyName)

-OffPeakDisconnectTimeout<Int32>

The number of minutes before the configured action should be performed after a user session disconnects outside peak hours.

Required?	false
Default Value	0

Accept Pipeline Input?	true (ByPropertyName)

-OffPeakExtendedDisconnectAction<SessionChangeHostingAction>

The action to be performed after a second configurable period of a user session disconnecting outside peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	Nothing
Accept Pipeline Input?	true (ByPropertyName)

-OffPeakExtendedDisconnectTimeout<Int32>

The number of minutes before the second configured action should be performed after a user session disconnects outside peak hours.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-OffPeakLogOffAction<SessionChangeHostingAction>

The action to be performed after a configurable period of a user session ending outside peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	Nothing
Accept Pipeline Input?	true (ByPropertyName)

-OffPeakLogOffTimeout<Int32>

The number of minutes before the configured action should be performed after a user session ends outside peak hours.

Required?	false
Default Value	0

Accept Pipeline Input?	true (ByPropertyName)

-PeakBufferSizePercent<Int32>

The percentage of machines in the desktop group that should be kept available in an idle state in peak hours.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-PeakDisconnectAction<SessionChangeHostingAction>

The action to be performed after a configurable period of a user session disconnecting in peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	Nothing
Accept Pipeline Input?	true (ByPropertyName)

-PeakDisconnectTimeout<Int32>

The number of minutes before the configured action should be performed after a user session disconnects in peak hours.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-PeakExtendedDisconnectAction<SessionChangeHostingAction>

The action to be performed after a second configurable period of a user session disconnecting in peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	Nothing

Accept Pipeline Input?	true (ByPropertyName)

-PeakExtendedDisconnectTimeout<Int32>

The number of minutes before the second configured action should be performed after a user session disconnects in peak hours.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-PeakLogOffAction<SessionChangeHostingAction>

The action to be performed after a configurable period of a user session ending in peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	Nothing
Accept Pipeline Input?	true (ByPropertyName)

-PeakLogOffTimeout<Int32>

The number of minutes before the configured action should be performed after a user session ends in peak hours.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-ProtocolPriority<String[]>

A list of protocol names in the order in which they should be attempted for use during connection.

Required?	false
Default Value	null

Accept Pipeline Input?	true (ByPropertyName)

-PublishedName<String>

The name that will be displayed to users for their desktop(s) in this desktop group.

Required?	false
Default Value	The same value as that supplied for the name of the desktop group.
Accept Pipeline Input?	true (ByPropertyName)

-Scope<String[]>

Specifies the name of the delegated administration scope to which the desktop group should belong.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-SecureIcaRequired<Boolean>

Whether HDX connections to desktops in the new desktop group require the use of a secure protocol.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-SessionSupport<SessionSupport>

Specifies whether machines in the desktop group are single or multi-session capable. Values can be:

o SingleSession - Single-session only machine.

o MultiSession - Multi-session capable machine.

Required?	false

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-SettlementPeriodBeforeAutoShutdown<TimeSpan>

Time after a session ends during which automatic shutdown requests (for example, shutdown after use, idle pool management) are deferred. Any outstanding shutdown request takes effect after the settlement period expires. This is typically used to configure time to allow logoff scripts to complete.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-ShutdownDesktopsAfterUse<Boolean>

Whether desktops in this desktop group should be automatically shut down when each user session completes (only relevant to power-managed desktops).

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-TimeZone<String>

The time zone in which this desktop group's machines reside.

The time zone must be specified for any of the group's automatic power management settings to take effect. Automatic power management operations include pool management (power time schemes), reboot schedules, session disconnect and logoff actions, and powering on assigned machines etc.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-TurnOnAddedMachine<Boolean>

This flag specifies whether the Broker Service should attempt to power on machines when they are added to the desktop group.

Required?	false
Default Value	$false for single session machines and $true for multi-session machines.
Accept Pipeline Input?	true (ByPropertyName)

-UUID<Guid>

An optional GUID for this desktop group.

Required?	false
Default Value	A new GUID is generated if none is supplied.
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.DesktopGroup

The newly created desktop group.

Notes

Once a new desktop group is created, you can create desktops in it by adding the appropriate broker machines to it using the Add-BrokerMachine or Add-BrokerMachinesToDesktopGroup cmdlets.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-BrokerDesktopGroup "Assigned Desktops" -PublishedName "MyDesktop" -DesktopKind Private
```

Create a desktop group to manage the brokering of private desktops, which will appear to users with the name "MyDesktop".

New-BrokerEntitlementPolicyRule

Sep 10, 2014

Creates a new desktop rule in the site's entitlement policy.

Syntax

New-BrokerEntitlementPolicyRule [-Name] <String> -DesktopGroupUid <Int32> [-ColorDepth <ColorDepth>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IconUid <Int32>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-PublishedName <String>] [-SecureIcaRequired <Boolean>] [-SessionReconnection <SessionReconnection>] [-UUID <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The New-BrokerEntitlementPolicyRule cmdlet adds a new desktop rule to the site's entitlement policy.

A desktop rule in the entitlement policy defines the users who are allowed per-session access to a machine from the rule's associated desktop group to run a full desktop session.

The following constraints apply when creating a desktop entitlement rule for a desktop group:

o The group's desktop kind must be Shared

o The group's delivery type must be DesktopsOnly or DesktopsAndApps

When a user selects a desktop entitlement published from a shared group, a machine is selected from the group on which to run the desktop session. No permanent association exists between the user and the selected machine; once the session ends the association also ends.

Multiple desktop rules in the entitlement policy can apply to the same desktop group. Where a user is granted an entitlement by more than one rule for the same group, they can use as many desktop sessions at the same time as they have entitlements.

Related topics

Get-BrokerEntitlementPolicyRule

Set-BrokerEntitlementPolicyRule

Rename-BrokerEntitlementPolicyRule

Remove-BrokerEntitlementPolicyRule

Parameters

-Name<String>

Specifies the administrative name of the new desktop rule. Each rule in the site's entitlement policy must have a unique name (irrespective of whether they are desktop or application rules).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroupUid<Int32>

Specifies the unique ID of the desktop group to which the new desktop rule applies.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ColorDepth<ColorDepth>

Specifies the color depth of any desktop sessions launched by a user from this entitlement.

Valid values are $null, FourBit, EightBit, SixteenBit, and TwentyFourBit.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Specifies an optional description of the new desktop rule. The text may be visible to the end user, for example, as a tooltip associated with the desktop entitlement.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Specifies whether the new desktop rule is initially enabled. A disabled rule is ignored when evaluating the site's entitlement policy.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUserFilterEnabled<Boolean>

Specifies whether the excluded users filter is initially enabled. If the filter is disabled then any user entries in the filter are ignored when entitlement policy rules are evaluated.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-ExcludedUsers<User[]>

Specifies the excluded users filter of the desktop rule, that is, the users and groups who are explicitly denied an entitlement to a desktop session from the new rule.

This can be used to exclude users or groups who would otherwise gain access by groups specified in the included users filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-IconUid<Int32>

Specifies the unique ID of the icon used to display the desktop session entitlement to the user.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUserFilterEnabled<Boolean>

Specifies whether the included users filter is initially enabled. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to a desktop session by the new rule.

Users who would be implicitly granted access when the filter is disabled can still be explicitly denied access using the excluded users filter.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-IncludedUsers<User[]>

Specifies the included users filter of the rule, that is, the users and groups who are granted an entitlement to a desktop session by the new rule.

If a user appears explicitly in the excluded users filter of the rule or is a member of a group that appears in the excluded users filter, no entitlement is granted whether or not the user appears in the included users filter.

Required?	false
Default Value	(empty list)
Accept Pipeline Input?	true (ByPropertyName)

-PublishedName<String>

The name of the new desktop session entitlement as seen by the user.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-SecureIcaRequired<Boolean>

Specifies whether the new desktop rule requires the SecureICA protocol for desktop sessions launched using the entitlement.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	null (dynamically inherited from the desktop group)
Accept Pipeline Input?	true (ByPropertyName)

-SessionReconnection<SessionReconnection>

Defines reconnection (roaming) behavior for sessions launched using this rule. Session reconnection control is an experimental and unsupported feature.

Required?	false
Default Value	Always
Accept Pipeline Input?	true (ByPropertyName)

-UUID<Guid>

An optional GUID for this rule.

Required?	false
Default Value	A new GUID is generated if none is supplied.
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.EntitlementPolicyRule

New-BrokerEntitlementPolicyRule returns the newly created desktop rule in the entitlement policy.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Customer Support'
C:\PS> New-BrokerEntitlementPolicyRule 'UK Office' -DesktopGroupUid $dg.Uid -IncludedUsers support\uk-staff -PublishedName 'Support Desktop'
```

Creates an desktop rule in the entitlement policy that entitles all members of the SUPPORT\uk-staff group to a desktop session from the Customer Support desktop group. The desktop entitlement name seen by users is Support Desktop.

New-BrokerHostingPowerAction

Sep 10, 2014

Creates a new action in the power action queue.

Syntax

```
New-BrokerHostingPowerAction [-MachineName] <String> -Action <PowerManagementAction> [-ActualPriority <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The New-BrokerHostingPowerAction cmdlet adds a new power action record into the queue of power actions to be performed. The power actions in the queue are processed on a priority basis and sent to the relevant hypervisor to change the power state of a virtual machine.

A power action record defines the action to be performed, the machine on which the action is to be performed, and an initial priority value for the action. Multiple actions may be created that relate to the same machine.

For a detailed description of the queuing mechanism, see 'help about_Broker_PowerManagement'.

Related topics

Get-BrokerHostingPowerAction

Set-BrokerHostingPowerAction

Remove-BrokerHostingPowerAction

Parameters

-MachineName<String>

Specifies the machine that the action is to be performed on.

The machine can be identified by DNS name or short name or SID or 'machine\domain' form name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Action<PowerManagementAction>

Specifies the power state change action that is to be performed on the specified machine.

Valid values are: TurnOn, TurnOff, ShutDown, Reset, Restart, Suspend and Resume.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ActualPriority<Int32>

Specifies an initial priority value for the action in the queue.

This priority is the current action priority; the 'base' priority for actions created via this cmdlet is always 30. Numerically lower priority values indicate more important actions that are processed in preference to actions with numerically higher priority settings.

Required?	false
Default Value	30
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.HostingPowerAction

New-BrokerHostingPowerAction returns the newly created power action record.

Examples

---------- EXAMPLE 1 ----------

C:\PS> New-BrokerHostingPowerAction -Action Shutdown -MachineName 'XD_VDA1'
Causes the machine called 'XD_VDA1' to be shut down.

New-BrokerHypervisorConnection

Sep 10, 2014

Creates a new hypervisor connection.

Syntax

New-BrokerHypervisorConnection [-HypHypervisorConnectionUid] <Guid> [-PreferredController <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The New-BrokerHypervisorConnection cmdlet creates a new hypervisor connection.

Related topics

Get-BrokerHypervisorConnection

Remove-BrokerHypervisorConnection

Set-BrokerHypervisorConnection

Parameters

-HypHypervisorConnectionUid<Guid>

The Guid that identifies the hypervisor connection, as defined in DUM.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PreferredController<String>

The preferred controller machine for the hypervisor connection. Can be specified as (first match is used):

o Full SAM name.

o Full DNS name.

o SID value.

o NetBIOS name (SAM without domain).

o Partial DNS name (DNS name without some or all domain information).

Where not specified, the system selects preferred controller machine based on loading.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.

Accept Pipeline Input?	false

Input Type

None

Return Values

Citrix.Broker.Admin.SDK.HypervisorConnection

New-BrokerHypervisorConnection returns an opaque object containing information about the hypervisor connection.

Examples

---------- EXAMPLE 1 ----------

C:\PS> New-BrokerHypervisorConnection -PreferredController "domainName\controllerName" -HypHypervisorConnectionUid "d16f4e56-b85e-4ba6-b745-0e978ae4f192"
This command creates a new hypervisor connection with a preferred controller.

---------- EXAMPLE 2 ----------

C:\PS> New-BrokerHypervisorConnection -HypHypervisorConnectionUid "d16f4e56-b85e-4ba6-b745-0e978ae4f192"
This command creates a new hypervisor connection, and leaves it to the system to select a preferred controller.

New-BrokerIcon

Sep 10, 2014

Creates a new icon.

Syntax

New-BrokerIcon [-EncodedIconData] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Accepts Base64 encoded .ICO format icon data, stores it in the database and returns an Icon object containing the Uid assigned to it.

New-BrokerIcon can be used with the Get-CtxIcon cmdlet from Citrix.Common.Commands, to obtain the Base64 icon. See Examples for a demonstration.

Related topics

Get-CtxIcon

Get-BrokerIcon

Remove-BrokerIcon

Parameters

-EncodedIconData<String>

Specifies the Base64 encoded .ICO format icon data.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None Input cannot be piped to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Icon

Returns an Icon object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Add-PSSnapin Citrix.Common.Commands
C:\PS> $ctxIcon = Get-CtxIcon -FileName C:\Windows\System32\notepad.exe -index 0
C:\PS> $brokerIcon = New-BrokerIcon -EncodedIconData $ctxIcon.EncodedIconData
C:\PS> $desktopGroup = Get-BrokerDesktopGroup -Name 'MyDesktopGroup'
C:\PS> Set-BrokerDesktopGroup $desktopGroup -IconUid $brokerIcon.Uid
```

Extracts the first icon resource from notepad.exe, and sets this as the icon for a desktop group.

New-BrokerMachine

Sep 10, 2014

Adds a machine that can be used to run desktops and applications.

Syntax

New-BrokerMachine [-MachineName] <String> -CatalogUid <Int32> [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-HostedMachineId <String>] [-HypervisorConnectionUid <Int32>] [-InMaintenanceMode <Boolean>] [-UUID <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

By adding a machine to a catalog, New-BrokerMachine adds a machine to the site, and is the first step in making the machine available to run users' desktops and applications. The machine may be physical or virtual.

For physical machines, you must specify the machine's SID and the catalog to which it will belong. For virtual machines which are not provisioned by MCS, you must also provide the hypervisor connection responsible for running the machine and the hosted machine ID by which the hypervisor recognizes the machine.

The machine must support the expected capabilities of the catalog: the catalog specifies a SessionType and a MinimalFunctionalLevel. The session support of the machine is determined by the type of Citrix VDA software installed (server or workstation) and the functional level depends on the version of the Citrix VDA software installed. The New-BrokerMachine command will complete successfully if these are not correct but the machine will be unable to register.

For more information about machines, see about_Broker_Machines.

Related topics

Add-BrokerMachine

Parameters

-MachineName<String>

Specify the name of the machine to create (in the form 'domain\machine'). A SID can also be specified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-CatalogUid<Int32>

The catalog to which this machine will belong.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-AssignedClientName<String>

The client name to which this machine will be assigned. Machines can be assigned to multiple users, a single client IP address, or a single client name, but only to one of these categories at a time.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-AssignedIPAddress<String>

The client IP address to which this machine will be assigned. Machines can be assigned to multiple users, a single client IP address, or a single client name, but only to one of these categories at a time.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-HostedMachineId<String>

The unique ID by which the hypervisor recognizes the machine. Omit this for physical machines or MCS-provisioned VMs.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-HypervisorConnectionUid<Int32>

The hypervisor connection that runs the machine. Omit this for physical machines or MCS-provisioned VMs.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-InMaintenanceMode<Boolean>

Specifies whether the machine is initially in maintenance mode. A machine in maintenance mode is not available for new sessions, and for managed machines all automatic power management is disabled.

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-UUID<Guid>

An optional GUID for this machine.

Required?	false
Default Value	A new GUID is generated if none is supplied.
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Machine

New-BrokerMachine returns the created machine.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-BrokerMachine -CatalogUid 2 -MachineName 'domain\machine'
```

This adds the physical machine with the specified SAM name to this site and places it in the specified catalog.

---------- EXAMPLE 2 ----------

```
C:\PS> New-BrokerMachine -CatalogUid 2 -MachineName 'S-1-5-12-1234567890-1234567890-1234567890-1234'
```

This adds the physical machine with the specified SID to this site and places it in the specified catalog.

---------- EXAMPLE 3 ----------

```
C:\PS> New-BrokerMachine -CatalogUid 2 -MachineName 'domain\machine' -HostedMachineId 'F8143B4F-7371-4efa-868A-54787EF9F64E' -HypervisorConnectionUid 5
```

This adds the virtual machine, running on the specified hypervisor, to this site and places it in the catalog.

---------- EXAMPLE 4 ----------

```
C:\PS> $m = New-BrokerMachine -CatalogUid 2 -MachineName 'domain\machine'
C:\PS> Add-BrokerMachine -InputObject $m -DesktopGroup 3
```

This adds the specified physical machine to the site and uses Add-BrokerMachine to add it to a desktop group.

New-BrokerMachineCommand

Sep 10, 2014

Creates a new command to deliver to a desktop.

Syntax

New-BrokerMachineCommand -User <String> -Category <String> -CommandName <String> [-DesktopGroups <DesktopGroup[]>] [-SendTrigger <MachineCommandTrigger>] [-SendDeadline <TimeSpan>] [-CommandData <Byte[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-BrokerMachineCommand -SessionUid <Int64> -Category <String> -CommandName <String> [-SendTrigger <MachineCommandTrigger>] [-SendDeadline <TimeSpan>] [-CommandData <Byte[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-BrokerMachineCommand -MachineUid <Int32> -Category <String> -CommandName <String> [-SendTrigger <MachineCommandTrigger>] [-SendDeadline <TimeSpan>] [-CommandData <Byte[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-BrokerMachineCommand -Synchronous -MachineUid <Int32> -Category <String> -CommandName <String> [-CommandData <Byte[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Create a new command queued for delivery to a desktop. Commands are sent to a specific handler installed on the desktop using the Category parameter. Each handler has its own list of commands identified by the CommandName parameter. Optional command data can be provided using the CommandData parameter in a format specified by the handler.

Commands are targeted at a specific user, session or machine. Commands targeted at a user can be further be restricted to one or more desktop groups.

The SendTrigger is used to restrict the command to a specific event related to the target. For example, when the target machine registers or when the target user reconnects to a session. The command will be sent to the machine when the SendTrigger occurs for the target.

If the Synchronous switch is provided, the target must be a machine and no SendTrigger can be specified. The command is sent immediately to the machine if it is currently registered and fails if the machine is not registered.

Note that the combined length of the Category and CommandName is limited to 64 characters. The Category and CommandName must both be entirely alphanumeric and not include any white space.

Related topics

Get-BrokerMachineCommand

Remove-BrokerMachineCommand

Parameters

-Category<String>

The service on the desktop to send the command to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-CommandName<String>

The name of the command to send (as defined by the service).

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-User<String>

User whose desktop or session should receive the command.

Required?	true
Default Value	Any user.
Accept Pipeline Input?	true (ByPropertyName)

-SessionUid<Int64>

Currently logged on user session that should receive the command.

Required?	true
Default Value	Any session.
Accept Pipeline Input?	true (ByPropertyName)

-MachineUid<Int32>

Specific machine that should receive the command.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Synchronous<SwitchParameter>

Send the command immediately and block while waiting for the reply.

Required?	true
Default Value	false
Accept Pipeline Input?	false

-CommandData<Byte[]>

Optional additional data to include with the command.

Required?	false
Default Value	None
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

-DesktopGroups<DesktopGroup[]>

Further restrict the command targeted at a user to machines in these desktop groups.

Required?	false
Default Value	No restriction by desktop group.
Accept Pipeline Input?	true (ByPropertyName)

-SendTrigger<MachineCommandTrigger>

Queue command for delivery until this particular event occurs. Valid values are NextContact, Broker, LogOn, Logoff, Disconnect and Reconnect.

Required?	false
Default Value	Default value is 'NextContact' so the command is sent during the next communication with the desktop.
Accept Pipeline Input?	true (ByPropertyName)

-SendDeadline<TimeSpan>

Automatically cancel the command if it not delivered before the specified time span passes.

Required?	false
Default Value	Command expires after 24 hours.
Accept Pipeline Input?	true (ByPropertyName)

Input Type

None No parameter is accepted from the input pipeline.

Return Values

Citrix.Broker.Admin.SDK.MachineCommand

New command that was added to the command queue.Citrix.Broker.Admin.SDK.MachineSynchronousCommandResponse

When the Synchronous option is used, the command is immediately sent to the specified machine and processed. The SDK object returned describes the command and the result of this command processing.

Notes

Commands are subject to delegated administration restrictions based on the desktop group, category and command name.

Examples

---------- EXAMPLE 1 ----------

```
New-BrokerMachineCommand -Category "UPM" -CommandName "ResetProfile" -DesktopGroups 1 -UserUid 23 -SendTrigger Authentication
```

Instruct the User Profile Manager service to execute the "ResetProfile" command when user 23 logs on to any machine in desktop group 1

---------- EXAMPLE 2 ----------

```
New-BrokerMachineCommand -Synchronous -Category "MonitorService" -CommandName "EnableLogging" -MachineUid 13
```

Instruct the monitor service to immediately execute the "EnableLogging" command on the machine having Uid 13.

New-BrokerMachineConfiguration

Sep 10, 2014

Creates a new machine configuration associated with an existing configuration slot.

Syntax

New-BrokerMachineConfiguration -ConfigurationSlotUid <Int32> -LeafName <String> -Policy <Byte[]> [-Description <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Creates a new machine configuration containing settings that match the SettingsGroup of the associated configuration slot. This machine configuration can then be applied to a desktop group to have the settings applied to machines in that group.

The SettingsGroup of the configuration slot restricts the permitted settings. Use the SDK snap-in that matches the SettingsGroup to create the encoded settings data.

Related topics

Get-BrokerMachineConfiguration

Set-BrokerMachineConfiguration

Rename-BrokerMachineConfiguration

Remove-BrokerMachineConfiguration

Add-BrokerMachineConfiguration

Parameters

-ConfigurationSlotUid<Int32>

Unique identifier of the configuration slot to associate with this machine configuration.

Required?	true
Default Value	None
Accept Pipeline Input?	true (ByPropertyName)

-LeafName<String>

Name of the new machine configuration. This must be unique amongst the machine configurations associated with the same configuration slot.

Required?	true
Default Value	None
Accept Pipeline Input?	true (ByPropertyName)

-Policy<Byte[]>

A binary array of encoded settings (policy) data created with the SDK snap-in that matches the SettingsGroup of the configuration slot.

Required?	true
Default Value	None
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Description of the new machine configuration.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a

series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.MachineConfiguration

New-BrokerMachineConfiguration returns the newly created configuration

Notes

Delegated Administration can be used to restrict the configuration slots that an administrator can use and hence which components of the system that can be configured.

Examples

---------- EXAMPLE 1 ----------

```
New-BrokerMachineConfiguration -LeafName "Finance Department" -Description "Finance Dept. User Profile Management policy" -Policy $policy -ConfigurationSlotUid $csl
```

Creates a new configuration named "%SlotName%\Finance Department" where %SlotName% is the name of the configuration slot having the Uid $csUid. The encoded settings in the $policy variable must match the SettingsGroup of the configuration slot having the Uid $csUid.

New-BrokerPowerTimeScheme

Sep 10, 2014

Creates a new power time scheme for a desktop group.

Syntax

New-BrokerPowerTimeScheme [-Name] <String> -DaysOfWeek <TimeSchemeDays> -DesktopGroupUid <Int32> [-DisplayName <String>] [-PeakHours <Boolean[]>] [-PoolSize <Int32[]>] [-PoolUsingPercentage <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The New-BrokerPowerTimeScheme cmdlet adds a new power time scheme to be associated with a desktop group. The power time scheme must relate to days of the week that are not already covered by an existing power time scheme.

Each power time scheme is associated with a particular desktop group, and covers one or more days of the week, defining which hours of those days are considered peak times and which are off-peak times. In addition, the time scheme defines a pool size value for each hour of the day for the days of the week covered by the time scheme. No one desktop group can be associated with two or more time schemes that cover the same day of the week.

See 'help about_Broker_PowerManagement' for a detailed description of the power policy mechanism and pool size management.

Related topics

Get-BrokerPowerTimeScheme

Set-BrokerPowerTimeScheme

Remove-BrokerPowerTimeScheme

Rename-BrokerPowerTimeScheme

Parameters

-Name<String>

Specifies the administrative name of the new power time scheme. Each scheme must have a name which is unique within the site.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DaysOfWeek<TimeSchemeDays>

Specifies the pattern of days of the week that the power time scheme covers.

Valid values are (singly or a list of) Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Weekdays and Weekend.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroupUid<Int32>

Specifies the desktop group that the power time scheme applies to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DisplayName<String>

Specifies the name of the new power time scheme as displayed in the DesktopStudio console. Each scheme associated with a desktop group must have a display name which is unique within its desktop group, although the same display name can be used on power schemes for different desktop groups.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PeakHours<Boolean[]>

A set of 24 boolean flag values, one for each hour of the day. The first value in the array relates to midnight to 00:59, the next one to 1 AM to 01:59 and so on, with the last array element relating to 11 PM to 11:59. If the flag is $true it means that the associated hour of the day is considered a peak time; if $false it means that it is considered off-peak.

Required?	false
Default Value	24 $false values, meaning all hours are off-peak
Accept Pipeline Input?	true (ByPropertyName)

-PoolSize<Int32[]>

A set of 24 integer values, one for each hour of the day. The first value in the array relates to midnight to 00:59, the next one to 1 AM to 01:59 and so on, with the last array element relating to 11 PM to 11:59. The value defines the number of machines (either as an absolute number or a percentage of the machines in the desktop group) that are to be maintained in a running state, whether they are in use or not. A value of -1 has special meaning: pool size management does not apply during such hours.

Required?	false
Default Value	24 values of '-1', meaning no pool size management is to be performed
Accept Pipeline Input?	true (ByPropertyName)

-PoolUsingPercentage<Boolean>

A boolean flag to indicate whether the integer values in the pool size array are to be treated as absolute values (if this value is $false) or as percentages of the number of machines in the desktop group (if this value is $true).

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.PowerTimeScheme

New-BrokerPowerTimeScheme returns the newly created power time scheme.

Examples

---------- **EXAMPLE 1** ----------

```
C:\PS> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHours (0..23 | %{ $_ -gt 8 -and $_ -lt 18 } )
```

Creates a new scheme attached to the desktop group whose UID value is 3. This new scheme covers the weekend and Monday and Tuesday, and defines 'peak' hours as 9am to 17:59, with all other times being 'off-peak'. No pool size values are supplied, so all size values for all the hours default to -1.

New-BrokerRebootSchedule

Sep 10, 2014

Creates a new reboot schedule for a desktop group.

Syntax

New-BrokerRebootSchedule [-DesktopGroupName] <String> -RebootDuration <Int32> [-Day <RebootScheduleDays>] [-Enabled <Boolean>] [-Frequency <RebootScheduleFrequency>] [-StartTime <TimeSpan>] [-WarningDuration <Int32>] [-WarningMessage <String>] [-WarningTitle <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-BrokerRebootSchedule -DesktopGroupUid <Int32> -RebootDuration <Int32> [-Day <RebootScheduleDays>] [-Enabled <Boolean>] [-Frequency <RebootScheduleFrequency>] [-StartTime <TimeSpan>] [-WarningDuration <Int32>] [-WarningMessage <String>] [-WarningTitle <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The New-BrokerRebootSchedule cmdlet is used to define a reboot schedule for a desktop group.

Related topics

Get-BrokerRebootSchedule

Set-BrokerRebootSchedule

Remove-BrokerRebootSchedule

Start-BrokerRebootCycle

Parameters

-DesktopGroupName<String>

The name of the desktop group that this reboot schedule is applied to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-RebootDuration<Int32>

Approximate maximum number of minutes over which the scheduled reboot cycle runs.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroupUid<Int32>

The Uid of the desktop group that this reboot schedule is applied to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Day<RebootScheduleDays>

For weekly schedules, the day of the week on which the scheduled reboot-cycle starts (one of Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday).

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Boolean that indicates if the new reboot schedule is enabled.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Frequency<RebootScheduleFrequency>

Frequency with which this schedule runs (either Weekly or Daily).

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-StartTime<TimeSpan>

Time of day at which the scheduled reboot cycle starts (HH:MM).

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-WarningDuration<Int32>

Time prior to the initiation of a machine reboot at which warning message is displayed in all user sessions on that machine. If the warning duration is zero then no message is displayed.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-WarningMessage<String>

Warning message displayed in user sessions on a machine scheduled for reboot. If the message is blank then no message is displayed.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-WarningTitle<String>

The window title used when showing the warning message in user sessions on a machine scheduled for reboot.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None Input cannot be piped to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.RebootSchedule

Examples

---------- EXAMPLE 1 ----------

C:\PS> New-BrokerRebootSchedule -DesktopGroupName BankTellers -Frequency Daily -StartTime "02:00" -Enabled $true -Duration 120
Schedules the machines in the desktop group named 'BankTellers' to be rebooted every night between 2 AM and 4 AM.

---------- EXAMPLE 2 ----------

C:\PS> New-BrokerRebootSchedule -DesktopGroupUid 17 -Frequency Weekly -Day Saturday -StartTime "01:00" -Enabled $true -Duration 240 -WarningTitle "WARNING: Rebo
Schedules the machines in the desktop group having Uid 17 to be rebooted every Saturday night between 1 AM and 5 AM. Ten minutes prior to rebooting, each machine will display a message box with the title "WARNING: Reboot pending" and message "Save your work" in every user session.

New-BrokerRemotePCAccount

Sep 10, 2014

Create a new RemotePCAccount.

Syntax

New-BrokerRemotePCAccount -CatalogUid <Int32> -OU <String> [-AllowSubfolderMatches <Boolean>] [-MachinesExcluded <String[]>] [-MachinesIncluded <String[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Create a new RemotePCAccount. A RemotePCAccount defines machine filters to support Remote PC automation adding unconfigured machines to catalogs.

Related topics

Get-BrokerRemotePCAccount

Set-BrokerRemotePCAccount

Remove-BrokerRemotePCAccount

Parameters

-CatalogUid<Int32>

Specifies the catalog which Remote PC automation adds an unconfigured machine to if it matches this RemotePCAccount.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-OU<String>

Specifies the DN of an AD container, or has the special value 'any'.

When an AD container is specified a machine may only match with the RemotePCAccount when the AD computer object is located relative to the OU.

When 'any' is specified the location of the AD computer object is ignored for purposes of matching this RemotePCAccount. The machine must still meet the MachinesIncluded and MachinesExcluded filters for a match to occur.

In the event that a machine matches with multiple RemotePCAccounts then the RemotePCAccount OU with the longest canonical name takes precedence. The special 'any' OU is treated as lowest priority.

Note that the OU value of every RemotePCAccount must be unique, and this includes only one 'any' entry being permitted.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-AllowSubfolderMatches<Boolean>

When true a machine matches this RemotePCAccount if the AD computer object exists within the container specified by the OU property, or within a child container of the OU.

When false the AD computer object only matches if it exists directly in the AD container specified by the OU property.

This property is not meaningful when OU has the special value 'any'.

Required?	false
Default Value	false

Accept Pipeline Input?	true (ByPropertyName)

-MachinesExcluded<String[]>

MachinesExcluded specifies a set of strings that can include asterisk wildcards. If a machine name matches any entries in MachinesExcluded then it cannot match with this RemotePCAccount regardless of whether there is a MachinesIncluded match.

Matches are performed against the domain name joined with the machine name by a backslash (DOMAIN\MACHINE), e.g.:

DOMAIN1\M*

DOMAIN*\M*

\M

Required?	false
Default Value	@()
Accept Pipeline Input?	true (ByPropertyName)

-MachinesIncluded<String[]>

MachinesIncluded specifies a set of strings that can include asterisk wildcards. A machine may only match with this RemotePCAccount if it matches a MachinesIncluded entry and does not match any MachinesExcluded entries.

Matches are performed against the domain name joined with the machine name by a backslash (DOMAIN\MACHINE), e.g.:

DOMAIN1\M*

DOMAIN*\M*

\M

Required?	false
Default Value	@('*')
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.RemotePCAccount

The newly created RemotePCAccount.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-BrokerRemotePCAccount -OU 'ou=MyOU,dc=MyDomain,dc=com' -CatalogUid 42
```

Create a RemotePCAccount that adds unconfigured machines with computer objects in MyOU, into catalog 42.

---------- EXAMPLE 2 ----------

```
C:\PS> New-BrokerRemotePCAccount -OU 'any' -CatalogUid 42 -MachinesIncluded @('DOMAIN1\*') -MachinesExcluded @('DOMAIN1\*JOHNDOE*')
```

Create a RemotePCAccount matching unconfigured machines from DOMAIN1, except those with hostnames containing JOHNDOE, and add them to catalog 42.

---------- EXAMPLE 3 ----------

```
C:\PS> New-BrokerRemotePCAccount -OU 'any' -CatalogUid 42
```

Create a RemotePCAccount that matches any unconfigured machine, causing automation to add matching machines to catalog 42.

New-BrokerSessionLinger

Sep 10, 2014

Creates a new session linger setting for a desktop group.

Syntax

```
New-BrokerSessionLinger [-DesktopGroupName] <String> [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
New-BrokerSessionLinger -DesktopGroupUid <Int32> [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The New-BrokerSessionLinger cmdlet is used to define a session linger setting for a desktop group.

Note that each desktop group can only have a single session linger setting. Session lingering only applies to application sessions.

Related topics

Get-BrokerSessionLinger

Set-BrokerSessionLinger

Remove-BrokerSessionLinger

Parameters

-DesktopGroupName<String>

The name of the desktop group that this linger setting is applied to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroupUid<Int32>

The Uid of the desktop group that this linger setting is applied to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Boolean that indicates if the new session linger is enabled.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-MaxAverageLoadThreshold<Int32>

Specifies the average load threshold across the desktop group. When the threshold hits, lingering sessions across the group be terminated to reduce load. Sessions that have been lingering the longest will be chosen first.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-MaxLoadPerMachineThreshold<Int32>

Specifies the maximum load threshold per machine in the desktop group. When the threshold hits, lingering sessions on each loaded machine will be terminated to reduce load. Sessions that have been lingering the longest will be chosen first.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-MaxTimeBeforeDisconnect<TimeSpan>

Specifies the time by which a lingering session will be disconnected. The disconnect timer is optional, but when specified the terminate timer needs to be also set. The disconnect time cannot be greater than the terminate time. When the disconnect and terminate times are the same, the terminate timer takes precedence. The disconnect timer needs to be paired with a session termination condition like the terminate timer or one of load threshold settings.

Required?	false
Default Value	15 minutes
Accept Pipeline Input?	true (ByPropertyName)

-MaxTimeBeforeTerminate<TimeSpan>

Specifies the time by which a lingering session will be terminated. The terminate timer is not optional when timers are configured. When the disconnect and terminate times are the same, the terminate timer takes precedence.

Required?	false
Default Value	8 hours
Accept Pipeline Input?	true (ByPropertyName)

-UserFilterEnabled<Boolean>

Specifies whether the session linger's user filter is enabled or disabled. Where the user filter is enabled, lingering is enabled only to users who appear in the filter (either explicitly or by virtue of group membership).

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Depends on parameter Parameters can be piped by property name.

Return Values

Citrix.Broker.Admin.SDK.SessionLinger

New-BrokerSessionLinger returns a session linger object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> New-BrokerSessionLinger -DesktopGroupName test -Enabled $true -MaxTimeBeforeDisconnect 0:30 -MaxTimeBeforeTerminate 1:00
Creates a new session linger setting with a disconnect timer of 30 minutes and terminate timer of 1 hour.

New-BrokerSessionPreLaunch

Sep 10, 2014

Creates a new session pre-launch setting for a desktop group.

Syntax

```
New-BrokerSessionPreLaunch [-DesktopGroupName] <String> [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
New-BrokerSessionPreLaunch -DesktopGroupUid <Int32> [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The New-BrokerSessionPreLaunch cmdlet is used to define a session pre-launch setting for a desktop group.

Note that each desktop group can only have a single session pre-launch setting. Session pre-launch only applies to application sessions.

Related topics

Get-BrokerSessionPreLaunch

Set-BrokerSessionPreLaunch

Remove-BrokerSessionPreLaunch

Parameters

-DesktopGroupName<String>

The name of the desktop group that this pre-launch setting is applied to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroupUid<Int32>

The Uid of the desktop group that this pre-launch setting is applied to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Boolean that indicates if the new session pre-launch is enabled.

Required?	false
Default Value	true
Accept Pipeline Input?	true (ByPropertyName)

-MaxAverageLoadThreshold<Int32>

Specifies the average load threshold across the desktop group. When the threshold hits, pre-launched sessions across the group be terminated to reduce load. Sessions that have been pre-launched the longest will be chosen first.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-MaxLoadPerMachineThreshold<Int32>

Specifies the maximum load threshold per machine in the desktop group. When the threshold hits, pre-launched sessions on each loaded machine will be terminated to reduce load. Sessions that have been pre-launched the longest will be chosen first.

Required?	false
Default Value	0
Accept Pipeline Input?	true (ByPropertyName)

-MaxTimeBeforeDisconnect<TimeSpan>

Specifies the time by which a pre-launched session will be disconnected. The disconnect timer is optional, but when specified the terminate timer needs to be also set. The disconnect time cannot be greater than the terminate time. When the disconnect and terminate times are the same, the terminate timer takes precedence. The disconnect timer needs to be paired with a session termination condition like the terminate timer or one of load threshold settings.

Required?	false
Default Value	15 minutes
Accept Pipeline Input?	true (ByPropertyName)

-MaxTimeBeforeTerminate<TimeSpan>

Specifies the time by which a pre-launched session will be terminated. The terminate timer is not optional when timers are configured. When the disconnect and terminate times are the same, the terminate timer takes precedence.

Required?	false
Default Value	8 hours
Accept Pipeline Input?	true (ByPropertyName)

-UserFilterEnabled<Boolean>

Specifies whether the session pre-launch's user filter is enabled or disabled. Where the user filter is enabled, pre-launch is enabled only to users who appear in the filter (either explicitly or by virtue of group membership).

Required?	false
Default Value	false
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Depends on parameter Parameters can be piped by property name.

Return Values

Citrix.Broker.Admin.SDK.SessionPreLaunch

New-BrokerSessionPreLaunch returns a session pre-launch object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> New-BrokerSessionPreLaunch -DesktopGroupName test -Enabled $true -MaxTimeBeforeDisconnect 0:30 -MaxTimeBeforeTerminate 1:00
Creates a new session pre-launch setting with a disconnect timer of 30 minutes and terminate timer of 1 hour.

New-BrokerTag

Sep 10, 2014

Creates a new tag.

Syntax

New-BrokerTag [-Name] <String> [-UUID <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Creates a tag that can be associated with other objects using Add-BrokerTag.

Related topics

Add-BrokerTag

Get-BrokerTag

Remove-BrokerTag

Rename-BrokerTag

Parameters

-Name<String>

Specifies a name for the new tag.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-UUID<Guid>

Specifies a UUID for the new tag. When not specified, a UUID is automatically assigned.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None Input cannot be piped to this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.Tag

Outputs the generated tag.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-BrokerTag -Name 'Tag1'
```
Creates a new tag with name 'Tag1'.

---------- EXAMPLE 2 ----------

```
C:\PS> New-BrokerTag 'Tag2' | Add-BrokerTag -Desktop $desktop
```
Creates a new tag with name 'Tag2' and associates it with Desktop $desktop.

New-BrokerUser

Sep 10, 2014

Creates a new broker user object

Syntax

```
New-BrokerUser [-SID] <SecurityIdentifier> [-AdminAddress <String>] [<CommonParameters>]

New-BrokerUser [-Name] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The New-BrokerUser cmdlet creates a new broker object to represent a user identity (or the identity of a group of users). The object is created local to the PowerShell environment in which the cmdlet is run; no new user object is created in the broker configuration, unless the object is added to another broker object, such as a machine or a desktop. For details, see Add-BrokerUser.

The identity of the user or group must be specified using either the Name or SID parameter

Related topics

Add-BrokerUser

Get-BrokerUser

Remove-BrokerUser

Parameters

-SID<SecurityIdentifier>

The SID of the user or group

Required?	true
Default Value	null
Accept Pipeline Input?	false

-Name<String>

The name of the user or group

Required?	true
Default Value	null

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Broker.Admin.SDK.User

The broker user object

Notes

Typically, broker user objects are created implicitly using the Add-BrokerUser cmdlet with a user name or SID.

Examples

---------- EXAMPLE 1 ----------

```
$user = New-BrokerUser DOMAIN\UserName
```

Create a broker user object for the specified user.

---------- EXAMPLE 2 ----------

```
$user = New-BrokerUser -SID S-1-5-23-1763203430-193137401-908696819-3450
```

Create a broker user object for the specified user.

Remove-BrokerAccessPolicyRule

Sep 10, 2014

Deletes a rule from the site's access policy.

Syntax

```
Remove-BrokerAccessPolicyRule [-InputObject] <AccessPolicyRule[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerAccessPolicyRule [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerAccessPolicyRule cmdlet deletes a rule from the site's access policy.

An access policy rule defines a set of connection filters and access control rights relating to a desktop group. These allow fine-grained control of what access is granted to a desktop group based on details of, for example, a user's endpoint device, its address, and the user's identity.

Deleting a rule does not affect existing user sessions, but it may result in users being unable to launch new sessions, or reconnect to disconnected sessions if access to the desktop group delivering those sessions was granted by the deleted rule.

Related topics

New-BrokerAccessPolicyRule

Get-BrokerAccessPolicyRule

Set-BrokerAccessPolicyRule

Rename-BrokerAccessPolicyRule

Parameters

-InputObject<AccessPolicyRule[]>

The access policy rule to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the access policy rule to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AccessPolicyRule The access policy rule to be deleted.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerAccessPolicyRule 'Temp Staff'
```

Deletes the access policy rule called Temp Staff. Existing sessions are not affected, but if access was granted by the deleted rule users may be unable to reconnect to sessions if they are subsequently disconnected.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerAccessPolicyRule -IncludedUsers sales\johndoe | Remove-BrokerAccessPolicyRule
```

Deletes all access policy rules explicitly granting user SALES\johndoe access to any desktop group in the site. Any existing desktop sessions for the user are not affected. The user may still be able to access site resources by access policy rules that grant access through group membership or non-user-based connection filters.

Remove-BrokerAccessPolicyRuleMetadata

Sep 10, 2014

Deletes AccessPolicyRule Metadata from the AccessPolicyRule objects

Syntax

```
Remove-BrokerAccessPolicyRuleMetadata [-InputObject] <AccessPolicyRule[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerAccessPolicyRuleMetadata cmdlet deletes Metadata from the AccessPolicyRule objects.

Related topics

Parameters

-InputObject<AccessPolicyRule[]>

Specifies the AccessPolicyRule object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerAccessPolicyRule You can pipe the AccessPolicyRule to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerAccessPolicyRuleMetadata -InputObject $obj-Uid -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for the AccessPolicyRule whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerAccessPolicyRule | Remove-BrokerAccessPolicyRuleMetadata -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for all the AccessPolicyRule in the site

Remove-BrokerAdminFolder

Sep 10, 2014

Removes an admin folder.

Syntax

```
Remove-BrokerAdminFolder [-InputObject] <AdminFolder[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerAdminFolder [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerAdminFolder cmdlet removes an existing admin folder.

Remove-BrokerAdminFolder will not remove a folder if it contains any other objects (e.g. sub-folders or applications).

Related topics

Get-BrokerAdminFolder

New-BrokerAdminFolder

Parameters

-InputObject<AdminFolder[]>

Identifies the folder to remove

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name pattern of folder(s) to remove

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AdminFolder The admin folder objects can be specified as input.

Return Values

None

This cmdlet does not return any output.

Examples

---------- EXAMPLE 1 ----------

```
Remove-BrokerAdminFolder F1\F2\
```

Removes the folder called F2 within the folder F1\

Remove-BrokerAdminFolderMetadata

Sep 10, 2014

Deletes AdminFolder Metadata from the AdminFolder objects

Syntax

```
Remove-BrokerAdminFolderMetadata [-InputObject] <AdminFolder[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerAdminFolderMetadata cmdlet deletes Metadata from the AdminFolder objects.

Related topics

Parameters

-InputObject<AdminFolder[]>

Specifies the AdminFolder object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerAdminFolder You can pipe the AdminFolder to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerAdminFolderMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the AdminFolder whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerAdminFolder | Remove-BrokerAdminFolderMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the AdminFolder in the site

Remove-BrokerAppAssignmentPolicyRule

Sep 10, 2014

Deletes an application rule from the site's assignment policy.

Syntax

Remove-BrokerAppAssignmentPolicyRule [-InputObject] <AppAssignmentPolicyRule[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerAppAssignmentPolicyRule [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerAppAssignmentPolicyRule cmdlet deletes an application rule from the site's assignment policy.

An application rule in the assignment policy defines the users who are entitled to a self-service persistent machine assignment from the rule's desktop group; once assigned the machine can run one or more applications published from the group.

Deleting an application rule does not remove machine assignments that have already been made by the rule, nor does it affect active sessions to those machines in any way.

Related topics

New-BrokerAppAssignmentPolicyRule

Get-BrokerAppAssignmentPolicyRule

Set-BrokerAppAssignmentPolicyRule

Rename-BrokerAppAssignmentPolicyRule

Parameters

-InputObject<AppAssignmentPolicyRule[]>

The application rule to be deleted from the assignment policy.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the application rule to be deleted from the assignment policy.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AppAssignmentPolicyRule The application rule to be deleted from the assignment policy.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerAppAssignmentPolicyRule 'Temp Staff'
```

Deletes the application rule called Temp Staff from the assignment policy. Access to machines already assigned by this rule is not affected in any way.

---------- EXAMPLE 2 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Sales Support'
C:\PS> Get-BrokerAppAssignmentPolicyRule -DesktopGroupUid $dg.Uid | Remove-BrokerAppAssignmentPolicyRule
```

Deletes the application rule for the Sales Support desktop group from the site's assignment policy. This prevents any further machine assignments being made from this group, but it does not affect existing assignments made by the rule.

Remove-BrokerAppEntitlementPolicyRule

Sep 10, 2014

Deletes an application rule from the site's entitlement policy.

Syntax

```
Remove-BrokerAppEntitlementPolicyRule [-InputObject] <AppEntitlementPolicyRule[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerAppEntitlementPolicyRule [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerAppEntitlementPolicyRule cmdlet deletes an application rule from the site's entitlement policy.

An application rule in the entitlement policy defines the users who are allowed per-session access to a machine to run one or more applications published from the rule's desktop group.

Deleting a rule does not affect existing sessions launched using the rule, but users cannot reconnect to those sessions if they are subsequently disconnected.

Related topics

New-BrokerAppEntitlementPolicyRule

Get-BrokerAppEntitlementPolicyRule

Set-BrokerAppEntitlementPolicyRule

Rename-BrokerAppEntitlementPolicyRule

Parameters

-InputObject<AppEntitlementPolicyRule[]>

The application rule to be deleted from the entitlement policy.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the application rule to be deleted from the entitlement policy.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AppEntitlementPolicyRule The application rule to be deleted from the entitlement policy.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerAppEntitlementPolicyRule 'Temp Workers'
```

Deletes the application rule called Temp Workers from the entitlement policy rule. Existing application sessions launched using that rule are not affected, but users cannot reconnect to those sessions if they are subsequently disconnected.

---------- EXAMPLE 2 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Customer Support'
C:\PS> Get-BrokerAppEntitlementPolicyRule -DesktopGroupUid $dg.Uid | Remove-BrokerAppEntitlementPolicyRule
```

Deletes the application rule from the entitlement policy rule applied to the Customer Support desktop group. This effectively removes all access to the applications published from this group. Existing application sessions are not affected, but users cannot reconnect to those sessions if they are subsequently disconnected.

Remove-BrokerApplication

Sep 10, 2014

Deletes one or more applications, or an association of an application.

Syntax

```
Remove-BrokerApplication [-InputObject] <Application[]> [-Force] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerApplication [-Name] <String> [-Force] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerApplication cmdlet deletes one or more applications, or you can use it to delete just the association of an application to a desktop group.

Its usage dictates the behavior of the cmdlet. If only the application is specified as a parameter, then the cmdlet deletes the application. It also deletes any associations this application has with other objects, such as with access policy rules or desktop groups. More specifically, when an application is deleted the following happens:

o The association to any desktop groups is removed.

o The association to any tags is removed.

o Any configured file-type association objects for this application are deleted.

o The association to any user accounts is removed.

o The association to any access session conditions is removed.

o The access policy rule object for this application, if one existed, is deleted.

o Finally, the application object itself is deleted.

Note that if the application is in use by a user then the application cannot be deleted.

If more than just the application is supplied as a parameter to the cmdlet (for instance, if a DesktopGroup object is also specified) then the application is not deleted. Instead, only the association from the application to that desktop group is removed.

Related topics

New-BrokerApplication

Add-BrokerApplication

Get-BrokerApplication

Rename-BrokerApplication

Move-BrokerApplication

Parameters

-InputObject<Application[]>

Specifies the applications to delete. The Uid can also be substituted for the application objects.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the application to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Force<SwitchParameter>

Remove application even if it's in use. Removing an application that is currently in use, can potentially leave an application session containing no applications. If all the applications that are currently active in a disconnected application session are removed, the user will be unable to reconnect to the session. Forcing removal of an in-use application does not impact the actual session itself.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-DesktopGroup<DesktopGroup>

Specifies the desktop group that this application should no longer be associated with. The Uid or Name can also be substituted for the desktop group object.

Required?	false

Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Application The application objects can be specified as input.

Return Values

None

This cmdlet does not return any output.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerApplication "Notepad"
```

This command deletes the application that has a BrowserName of "Notepad".

---------- EXAMPLE 2 ----------

```
C:\PS> $app = Get-BrokerApplication -BrowserName "Notepad"
C:\PS> $group = Get-BrokerDesktopGroup -Name "Private DesktopGroup"
C:\PS> Remove-BrokerApplication -InputObject $app -DesktopGroup $group
```

This command removes the association of the desktop group that has a name of "Private DesktopGroup" from the application that has a BrowserName of "Notepad". It does not otherwise modify the application.

Remove-BrokerApplicationInstanceMetadata

Sep 10, 2014

Deletes ApplicationInstance Metadata from the ApplicationInstance objects

Syntax

```
Remove-BrokerApplicationInstanceMetadata [-InputObject] <ApplicationInstance[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerApplicationInstanceMetadata cmdlet deletes Metadata from the ApplicationInstance objects.

Related topics

Parameters

-InputObject<ApplicationInstance[]>

Specifies the ApplicationInstance object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerApplicationInstance You can pipe the ApplicationInstance to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerApplicationInstanceMetadata -InputObject $obj-Uid -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for the ApplicationInstance whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerApplicationInstance | Remove-BrokerApplicationInstanceMetadata -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for all the ApplicationInstance in the site

Remove-BrokerApplicationMetadata

Sep 10, 2014

Deletes Application Metadata from the Application objects

Syntax

```
Remove-BrokerApplicationMetadata [-InputObject] <Application[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerApplicationMetadata cmdlet deletes Metadata from the Application objects.

Related topics

Parameters

-InputObject<Application[]>

Specifies the Application object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerApplication You can pipe the Application to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerApplicationMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the Application whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerApplication | Remove-BrokerApplicationMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the Application in the site

Remove-BrokerAssignmentPolicyRule

Sep 10, 2014

Deletes a desktop rule from the site's assignment policy.

Syntax

```
Remove-BrokerAssignmentPolicyRule [-InputObject] <AssignmentPolicyRule[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerAssignmentPolicyRule [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerAssignmentPolicyRule cmdlet deletes a desktop rule from the site's assignment policy.

A desktop rule in the assignment policy defines the users who are entitled to self-service persistent machine assignments from the rule's desktop group. A rule defines how many machines a user is allowed from the group for delivery of full desktop sessions.

Deleting a desktop rule does not remove machine assignments that have already been made by the rule, nor does it affect active sessions to those machines in any way.

Related topics

New-BrokerAssignmentPolicyRule

Get-BrokerAssignmentPolicyRule

Set-BrokerAssignmentPolicyRule

Rename-BrokerAssignmentPolicyRule

Parameters

-InputObject<AssignmentPolicyRule[]>

The desktop rule to be deleted from the assignment policy.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the desktop rule to be deleted from the assignment policy.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AssignmentPolicyRule The desktop rule to be deleted from the assignment policy.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerAssignmentPolicyRule 'Temp Staff'
```

Deletes the desktop rule called Temp Staff from the assignment policy. Access to machines already assigned by this rule is not affected in any way.

---------- EXAMPLE 2 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Sales Support'
C:\PS> Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid | Remove-BrokerAssignmentPolicyRule
```

Deletes all desktop rules for the Sales Support desktop group from the site's assignment policy. This prevents any further machine assignments being made from this group, but it does not affect existing assignments made by these rules.

Remove-BrokerAssignmentPolicyRuleMetadata

Sep 10, 2014

Deletes AssignmentPolicyRule Metadata from the AssignmentPolicyRule objects

Syntax

```
Remove-BrokerAssignmentPolicyRuleMetadata [-InputObject] <AssignmentPolicyRule[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerAssignmentPolicyRuleMetadata cmdlet deletes Metadata from the AssignmentPolicyRule objects.

Related topics

Parameters

-InputObject<AssignmentPolicyRule[]>

Specifies the AssignmentPolicyRule object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerAssignmentPolicyRule You can pipe the AssignmentPolicyRule to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerAssignmentPolicyRuleMetadata -InputObject $obj-Uid -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for the AssignmentPolicyRule whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerAssignmentPolicyRule | Remove-BrokerAssignmentPolicyRuleMetadata -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for all the AssignmentPolicyRule in the site

Remove-BrokerCatalog

Sep 10, 2014

Removes catalogs from the site.

Syntax

```
Remove-BrokerCatalog [-InputObject] <Catalog[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]

Remove-BrokerCatalog [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Remove catalogs from the site.

In order to remove a catalog from a site, the catalog must not contain machines. To remove a machine from a catalog use the Remove-BrokerMachine cmdlet. Note: in order to remove a machine from a catalog, it must not belong to a desktop group.

Related topics

New-BrokerCatalog

Get-BrokerCatalog

Rename-BrokerCatalog

Set-BrokerCatalog

New-BrokerDesktopGroup

Remove-BrokerDesktopGroup

Parameters

-InputObject<Catalog[]>

Specifies the catalog objects to delete.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the catalog to delete.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Catalog You can pipe the catalogs to be deleted to Remove-BrokerCatalog.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerCatalog -Name "MyCatalog"
C:\PS> Remove-BrokerCatalog -InputObject (Get-BrokerCatalog -Name "MyCatalog")
```

These commands delete the catalog with the name "MyCatalog".

---------- EXAMPLE 2 ----------

```
C:\PS> Remove-BrokerCatalog -Name 'test*'
```

This command deletes all catalogs with names beginning with "test".

---------- EXAMPLE 3 ----------

```
C:\PS> Get-BrokerCatalog -RemotePCDesktopGroupUid 42 | Remove-BrokerCatalog -RemotePCDesktopGroup 42
```

Remove all the Remote PC catalogs that are associated with desktop group 42. Note that this only breaks the Remote PC relationships and does not delete the desktop groups.

Remove-BrokerCatalogMetadata

Sep 10, 2014

Deletes Catalog Metadata from the Catalog objects

Syntax

```
Remove-BrokerCatalogMetadata [-InputObject] <Catalog[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerCatalogMetadata cmdlet deletes Metadata from the Catalog objects.

Related topics

Parameters

-InputObject<Catalog[]>

Specifies the Catalog object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerCatalog You can pipe the Catalog to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerCatalogMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the Catalog whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerCatalog | Remove-BrokerCatalogMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the Catalog in the site

Remove-BrokerConfigurationSlot

Sep 10, 2014

Removes a configuration slot.

Syntax

```
Remove-BrokerConfigurationSlot [-InputObject] <ConfigurationSlot[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerConfigurationSlot [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Removes a configuration slot from the site. All machine configurations associated with this slot are also removed.

Related topics

New-BrokerConfigurationSlot

Get-BrokerConfigurationSlot

Parameters

-InputObject<ConfigurationSlot[]>

Configuration slot to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Name of configuration slot to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Configuration slot to remove Configuration slots may be specified through pipeline input.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
Remove-BrokerConfigurationSlot -Name "User Profile Manager"
```

Remove the configuration slot named "User Profile Manager".

Remove-BrokerConfigurationSlotMetadata

Sep 10, 2014

Deletes ConfigurationSlot Metadata from the ConfigurationSlot objects

Syntax

```
Remove-BrokerConfigurationSlotMetadata [-InputObject] <ConfigurationSlot[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerConfigurationSlotMetadata cmdlet deletes Metadata from the ConfigurationSlot objects.

Related topics

Parameters

-InputObject<ConfigurationSlot[]>

Specifies the ConfigurationSlot object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerConfigurationSlot You can pipe the ConfigurationSlot to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerConfigurationSlotMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the ConfigurationSlot whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerConfigurationSlot | Remove-BrokerConfigurationSlotMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the ConfigurationSlot in the site

Remove-BrokerConfiguredFTA

Sep 10, 2014

Deletes one or more configured file type associations.

Syntax

Remove-BrokerConfiguredFTA [-InputObject] <ConfiguredFTA[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Deletes one or more file type associations configured for a published application. At least one configured file type association object must be specified.

Related topics

Get-BrokerConfiguredFTA

New-BrokerConfiguredFTA

Parameters

-InputObject<ConfiguredFTA[]>

Specifies the ConfiguredFTA objects to delete.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.ConfiguredFTA[] One or more ConfiguredFTA objects can be supplied as input.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $ftas = Get-BrokerConfiguredFTA -ExtensionName ".txt"
C:\PS> Remove-BrokerConfiguredFTA $ftas
```

Deletes all configured file type associations with an extension name of ".txt".

Remove-BrokerControllerMetadata

Sep 10, 2014

Deletes Controller Metadata from the Controller objects

Syntax

Remove-BrokerControllerMetadata [-InputObject] <Controller[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerControllerMetadata cmdlet deletes Metadata from the Controller objects.

Related topics

Parameters

-InputObject<Controller[]>

Specifies the Controller object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerController You can pipe the Controller to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerControllerMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the Controller whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerController | Remove-BrokerControllerMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the Controller in the site

Remove-BrokerDelayedHostingPowerAction

Sep 10, 2014

Cancels one or more delayed power actions.

Syntax

```
Remove-BrokerDelayedHostingPowerAction [-InputObject] <DelayedHostingPowerAction[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerDelayedHostingPowerAction [-MachineName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Removes one or more delayed power actions that have not yet been queued for execution.

Related topics

Get-BrokerDelayedHostingPowerAction

New-BrokerDelayedHostingPowerAction

Parameters

-InputObject<DelayedHostingPowerAction[]>

The power action to be cancelled.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MachineName<String>

Cancels only actions for machines whose name (of the form domain\machine) matches the specified string.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.DelayedHostingPowerAction The power action to be cancelled.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerHostingPowerAction -MachineName 'XD_VDA1'
```

Cancels any pending delayed power actions for the machine called XD_VDA1.

Remove-BrokerDesktopGroup

Sep 10, 2014

Remove desktop groups from the system or remove them from a Remote PC catalog.

Syntax

```
Remove-BrokerDesktopGroup [-InputObject] <DesktopGroup[]> [-Force] [-RemotePCCatalog <Catalog>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Remove-BrokerDesktopGroup [-Name] <String> [-Force] [-RemotePCCatalog <Catalog>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This cmdlet has 2 functions:

o Remove desktop groups from the system.

o Break Remote PC associations between desktop groups and a catalog.

The Remote PC relationships are used by Remote PC automation to determine which desktop groups a machine in a particular Remote PC catalog can be published to. The assignment policy rules belonging to those desktop groups also determines the set of users that are allowed to be assigned to machines from the catalog.

Related topics

Get-BrokerDesktopGroup

New-BrokerDesktopGroup

Set-BrokerDesktopGroup

Add-BrokerDesktopGroup

Rename-BrokerDesktopGroup

New-BrokerCatalog

Remove-BrokerCatalog

Parameters

-InputObject<DesktopGroup[]>

Specifies the desktop groups to remove.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the desktop group to remove.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-Force<SwitchParameter>

Remove desktop groups even if there are active sessions.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-RemotePCCatalog<Catalog>

When this parameter is specified, Remote PC desktop groups are removed from the specified Remote PC catalog.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.DesktopGroup You can pipe desktop groups to Remove-BrokerDesktopGroup.

Return Values

None

Notes

If a desktop group contains desktops when it is removed, these desktops are also removed (but the underlying broker machine remains).

A desktop group that still has active sessions cannot be removed unless the -Force switch is used.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerDesktopGroup EMEA*
Remove all desktop groups with names starting with "EMEA".

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerDesktopGroup -Enabled $false | Remove-BrokerDesktopGroup -Force
Remove all desktops that are currently disabled even if there are active sessions.

---------- EXAMPLE 3 ----------

C:\PS> Get-BrokerDesktopGroup -RemotePCCatalogUid 42 | Remove-BrokerDesktopGroup -RemotePCCatalog 42
Remove all the Remote PC desktop groups that are associated with catalog 42. Note that this only breaks the Remote PC relationships and does not delete the desktop groups.

Remove-BrokerDesktopGroupMetadata

Sep 10, 2014

Deletes DesktopGroup Metadata from the DesktopGroup objects

Syntax

```
Remove-BrokerDesktopGroupMetadata [-InputObject] <DesktopGroup[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerDesktopGroupMetadata cmdlet deletes Metadata from the DesktopGroup objects.

Related topics

Parameters

-InputObject<DesktopGroup[]>

Specifies the DesktopGroup object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerDesktopGroup You can pipe the DesktopGroup to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerDesktopGroupMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the DesktopGroup whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerDesktopGroup | Remove-BrokerDesktopGroupMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the DesktopGroup in the site

Remove-BrokerEntitlementPolicyRule

Sep 10, 2014

Deletes a desktop rule from the site's entitlement policy.

Syntax

```
Remove-BrokerEntitlementPolicyRule [-InputObject] <EntitlementPolicyRule[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerEntitlementPolicyRule [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerEntitlementPolicyRule cmdlet deletes a desktop rule from the site's entitlement policy.

A desktop rule in the entitlement policy defines the users who are allowed per-session access to a machine from the rule's associated desktop group to run a full desktop session.

Deleting a rule does not affect existing sessions launched using the rule, but users cannot reconnect to those sessions if they are subsequently disconnected.

Related topics

New-BrokerEntitlementPolicyRule

Get-BrokerEntitlementPolicyRule

Set-BrokerEntitlementPolicyRule

Rename-BrokerEntitlementPolicyRule

Parameters

-InputObject<EntitlementPolicyRule[]>

The desktop rule to be deleted from the entitlement policy.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the desktop rule to be deleted from the entitlement policy.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.EntitlementPolicyRule The desktop rule to be deleted from the entitlement policy.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerEntitlementPolicyRule 'Temp Workers'
```

Deletes the desktop rule called Temp Workers from the entitlement policy. Existing desktop sessions launched using the rule are not affected, but users cannot reconnect to sessions if they are subsequently disconnected.

---------- EXAMPLE 2 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup 'Customer Support'
C:\PS> Get-BrokerEntitlementPolicyRule -DesktopGroupUid $dg.Uid | Remove-BrokerEntitlementPolicyRule
```

Deletes all desktop rules from the entitlement policy applying to the Customer Support desktop group. This effectively removes all access to the desktops published from this group. Existing desktop sessions are not affected, but users cannot reconnect to sessions if they are subsequently disconnected.

Remove-BrokerEntitlementPolicyRuleMetadata

Sep 10, 2014

Deletes EntitlementPolicyRule Metadata from the EntitlementPolicyRule objects

Syntax

Remove-BrokerEntitlementPolicyRuleMetadata [-InputObject] <EntitlementPolicyRule[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerEntitlementPolicyRuleMetadata cmdlet deletes Metadata from the EntitlementPolicyRule objects.

Related topics

Parameters

-InputObject<EntitlementPolicyRule[]>

Specifies the EntitlementPolicyRule object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerEntitlementPolicyRule You can pipe the EntitlementPolicyRule to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerEntitlementPolicyRuleMetadata -InputObject $obj-Uid -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for the EntitlementPolicyRule whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerEntitlementPolicyRule | Remove-BrokerEntitlementPolicyRuleMetadata -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for all the EntitlementPolicyRule in the site

Remove-BrokerHostingPowerAction

Sep 10, 2014

Cancel one or more pending power actions.

Syntax

```
Remove-BrokerHostingPowerAction [-InputObject] <HostingPowerAction[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerHostingPowerAction [-MachineName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Causes one or more of the pending power actions in the queue to be marked as cancelled. The affected power actions are not sent to the hypervisor for processing, and take no further part in the queuing activity.

Power actions cannot be cancelled once they have started to be processed by the hypervisor.

Related topics

Get-BrokerHostingPowerAction

New-BrokerHostingPowerAction

Set-BrokerHostingPowerAction

Parameters

-InputObject<HostingPowerAction[]>

The power action to be cancelled.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MachineName<String>

Cancels only actions for machines whose name (of the form domain\machine) matches the specified string.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.HostingPowerAction The power action to be cancelled.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerHostingPowerAction -MachineName 'XD_VDA1'
```

Cancels any pending power actions for the machine called 'XD_VDA1'.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerHostingPowerAction -Filter { State -eq "Pending" -and RequestTime -gt "-00:05" } | Remove-BrokerHostingPowerAction
```

Cancels any pending power actions requested in the last five minutes.

Remove-BrokerHostingPowerActionMetadata

Sep 10, 2014

Deletes HostingPowerAction Metadata from the HostingPowerAction objects

Syntax

```
Remove-BrokerHostingPowerActionMetadata [-InputObject] <HostingPowerAction[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerHostingPowerActionMetadata cmdlet deletes Metadata from the HostingPowerAction objects.

Related topics

Parameters

-InputObject<HostingPowerAction[]>

Specifies the HostingPowerAction object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerHostingPowerAction You can pipe the HostingPowerAction to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerHostingPowerActionMetadata -InputObject $obj-Uid -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for the HostingPowerAction whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerHostingPowerAction | Remove-BrokerHostingPowerActionMetadata -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for all the HostingPowerAction in the site

Remove-BrokerHypervisorAlertMetadata

Sep 10, 2014

Deletes HypervisorAlert Metadata from the HypervisorAlert objects

Syntax

Remove-BrokerHypervisorAlertMetadata [-InputObject] <HypervisorAlert[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerHypervisorAlertMetadata cmdlet deletes Metadata from the HypervisorAlert objects.

Related topics

Parameters

-InputObject<HypervisorAlert[]>

Specifies the HypervisorAlert object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerHypervisorAlert You can pipe the HypervisorAlert to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerHypervisorAlertMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the HypervisorAlert whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerHypervisorAlert | Remove-BrokerHypervisorAlertMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the HypervisorAlert in the site

Remove-BrokerHypervisorConnection

Sep 10, 2014

Removes a hypervisor connection from the system.

Syntax

Remove-BrokerHypervisorConnection [-InputObject] <HypervisorConnection[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerHypervisorConnection [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Remove-BrokerHypervisorConnection removes a hypervisor connection from the system. A hypervisor connection cannot be removed if it's being used by a machine.

Related topics

Get-BrokerHypervisorConnection

Set-BrokerHypervisorConnection

New-BrokerHypervisorConnection

Parameters

-InputObject<HypervisorConnection[]>

Specifies the hypervisor connection object to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the hypervisor connection object to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.HypervisorConnection You can pipe the hypervisor connection to be removed to Remove-BrokerHypervisorConnection.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
c:\PS> Remove-BrokerHypervisorConnection -Name "Xen Server Connection"
```

This command removes a hypervisor connection by name.

---------- EXAMPLE 2 ----------

```
c:\PS> $hvConn = Get-BrokerHypervisorConnection -PreferredController "controllerName" -Name "Xen Server Connection"
c:\PS> Remove-BrokerHypervisorConnection -InputObject $hvConn
```

Gets a hypervisor connection by preferred controller and removes it.

Remove-BrokerHypervisorConnectionMetadata

Sep 10, 2014

Deletes HypervisorConnection Metadata from the HypervisorConnection objects

Syntax

```
Remove-BrokerHypervisorConnectionMetadata [-InputObject] <HypervisorConnection[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerHypervisorConnectionMetadata cmdlet deletes Metadata from the HypervisorConnection objects.

Related topics

Parameters

-InputObject<HypervisorConnection[]>

Specifies the HypervisorConnection object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerHypervisorConnection You can pipe the HypervisorConnection to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerHypervisorConnectionMetadata -InputObject $obj-Uid -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for the HypervisorConnection whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerHypervisorConnection | Remove-BrokerHypervisorConnectionMetadata -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for all the HypervisorConnection in the site

Remove-BrokerIcon

Sep 10, 2014

Remove an icon.

Syntax

```
Remove-BrokerIcon [-InputObject] <Icon[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Removes an icon from the database.

Related topics

Get-BrokerIcon

New-BrokerIcon

Set-BrokerIconMetadata

Parameters

-InputObject<Icon[]>

Specifies the icon to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Icon The icon to be removed can be piped into the cmdlet.

Return Values

None

Notes

Note that if the icon is currently in use, for example, as a desktop icon, it cannot be removed until the association is cleared.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerIcon 3
Removes the icon with Uid 3.

Remove-BrokerIconMetadata

Sep 10, 2014

Deletes Icon Metadata from the Icon objects

Syntax

```
Remove-BrokerIconMetadata [-InputObject] <Icon[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerIconMetadata cmdlet deletes Metadata from the Icon objects.

Related topics

Parameters

-InputObject<Icon[]>

Specifies the Icon object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerIcon You can pipe the Icon to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerIconMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the Icon whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerIcon | Remove-BrokerIconMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the Icon in the site

Remove-BrokerImportedFTA

Sep 10, 2014

Deletes one or more imported file type associations.

Syntax

Remove-BrokerImportedFTA -DesktopGroupUids <Int32[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Deletes all of the imported file type associations belonging to one or more desktop groups. At least one desktop group must be specified.

Imported file type associations are grouped together based on the desktop group of the machine from which they were imported. All file types for a desktop group are deleted. There is no mechanism for deleting a subset imported file type associations for a specific desktop group.

Imported file type associations are different from configured file type associations. Imported file type associations are lists of known file type associations for a given desktop group. Configured file type associations are those that are actually associated with published applications for the purposes of content redirection.

Related topics

Get-BrokerImportedFTA

Update-BrokerImportedFTA

Parameters

-DesktopGroupUids<Int32[]>

Deletes the imported file type associations belonging to specified desktop groups.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Int32[] An array of Uids for the desktop groups can be supplied as input. The desktop groups must be of the Private or Shared desktop kind.

Return Values

None

Notes

If an imported file type association is used to create a new configured file type association and the imported file type association is subsequently deleted, the configured file type association is not affected.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $dg = Get-BrokerDesktopGroup -Name "Sales VMs"
C:\PS> Remove-BrokerImportedFTA -DesktopGroupUids $dg.Uid
```

Deletes all imported file type associations belonging to the "Sales VMs" desktop group.

Remove-BrokerLease

Sep 10, 2014

Remove the specified lease in the Database.

Syntax

```
Remove-BrokerLease [-InputObject] <Lease[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]

Remove-BrokerLease [-Key] <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Marks the specified lease for deletion. Note that the lease is eventually fully deleted when enough time has been allowed for the deletion to propagate to all controller machines in the site, but is immediately removed from lease search results.

Related topics

Update-BrokerLocalLeaseCache

Remove-BrokerCache

Parameters

-InputObject<Lease[]>

Specifies the lease to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Key<String>

Specifies the lease key of the lease to remove. A pattern can be specified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Lease The lease to be removed can be piped into the cmdlet.

Return Values

None

This cmdlet does not return any output.

Notes

The lease is marked for deletion after this cmdlet is run. Note that the lease is eventually fully deleted when enough time has been allowed for the deletion to propagate to all controller machines in the site, but is immediately removed from lease search results.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $lease = Get-BrokerLease -Uid 1
C:\PS> Remove-BrokerLease $lease
```

Marks the specified lease for deletion.

Remove-BrokerLeaseMetadata

Sep 10, 2014

Deletes Lease Metadata from the Lease objects

Syntax

Remove-BrokerLeaseMetadata [-InputObject] <Lease[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerLeaseMetadata cmdlet deletes Metadata from the Lease objects.

Related topics

Parameters

-InputObject<Lease[]>

Specifies the Lease object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerLease You can pipe the Lease to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerLeaseMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the Lease whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerLease | Remove-BrokerLeaseMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the Lease in the site

Remove-BrokerMachine

Sep 10, 2014

Removes one or more machines from its desktop group or catalog.

Syntax

```
Remove-BrokerMachine [-InputObject] <Machine[]> [-Force] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerMachine [-MachineName] <String> [-Force] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerMachine cmdlet removes one or more machines from their desktop group or catalog. There are three forms:

o Use the -InputObject parameter to remove a single machine instance or array of instances from their desktop group or catalog.

o Use the -MachineName parameter to remove the single named machine from its group or catalog.

o Use pipelining to pipe machine instances to the command.

To remove machines from their desktop group use the -DesktopGroup parameter; the specified group must be the one that contains the machines. If more than one machine is being removed from its group they must all be members of the same group.

If the -DesktopGroup parameter is not used then the machines are removed from their catalog. Removing a machine from its catalog deletes the record of the machine from the Citrix Broker Service.

Machines cannot be removed from their catalog while they are members of a desktop group.

Related topics

Add-BrokerMachine

Get-BrokerMachine

Parameters

-InputObject<Machine[]>

An array of machines to be removed from their desktop group or catalog.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MachineName<String>

The name of the single machine to remove (must match the MachineName property of the machine).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Force<SwitchParameter>

Forces removal of machine from a desktop group even if it is still in use (that is, there are user sessions running on the machine). Forcing removal of a machine does not disconnect or logoff the user sessions.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroup<DesktopGroup>

The desktop group from which the machines are to be removed, specified by name, UID, or instance.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Machine You can pipe in the machines to be removed.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerMachine -InputObject $machine -DesktopGroup $desktopGroup
C:\PS> Remove-BrokerMachine -InputObject $machine -DesktopGroup 2
C:\PS> Remove-BrokerMachine $machine -DesktopGroup "MyDesktopGroup"
```

These all remove a single machine from a desktop group, identifying the group by instance, UID, or name.

---------- EXAMPLE 2 ----------

```
C:\PS> Remove-BrokerMachine -MachineName "DOMAIN\MyMachine" -DesktopGroup 2
C:\PS> Remove-BrokerMachine DOMAIN\MyMachine -DesktopGroup "MyDesktopGroup"
C:\PS> Remove-BrokerMachine DOMAIN\MyMachine -DesktopGroup $desktopGroup
```

These remove the machine called "DOMAIN\MyMachine" from its desktop group.

---------- EXAMPLE 3 ----------

```
C:\PS> Remove-BrokerMachine -MachineName DOMAIN\MyMachine
C:\PS> Remove-BrokerMachine "DOMAIN\MyMachine"
C:\PS> Remove-BrokerMachine $machine
```

These all remove a machine from its catalog.

---------- EXAMPLE 4 ----------

```
C:\PS> Get-BrokerMachine -Uid 3 | Remove-BrokerMachine -DesktopGroup $dg
C:\PS> Get-BrokerMachine -CatalogUid 4 | Remove-BrokerMachine
```

These find specific machines and remove them from their desktop group or catalog.

Remove-BrokerMachineCommand

Sep 10, 2014

Cancel a pending command queued for delivery to a desktop.

Syntax

```
Remove-BrokerMachineCommand [-InputObject] <MachineCommand[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Sets the state of a pending command queued for delivery to a desktop to Canceled. The command is not removed from the system.

Related topics

Get-BrokerMachineCommand

New-BrokerMachineCommand

Parameters

-InputObject<MachineCommand[]>

Commands to cancel.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.MachineCommand Commands to cancel.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
Get-BrokerMachineCommand | Remove-BrokerMachineCommand
```

Cancel all pending commands.

---------- EXAMPLE 2 ----------

```
Get-BrokerMachineCommand -Category "UPM" | Remove-BrokerMachineCommand
```

Cancel all pending commands that have the category "UPM".

Remove-BrokerMachineCommandMetadata

Sep 10, 2014

Deletes MachineCommand Metadata from the MachineCommand objects

Syntax

```
Remove-BrokerMachineCommandMetadata [-InputObject] <MachineCommand[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerMachineCommandMetadata cmdlet deletes Metadata from the MachineCommand objects.

Related topics

Parameters

-InputObject<MachineCommand[]>

Specifies the MachineCommand object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerMachineCommand You can pipe the MachineCommand to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerMachineCommandMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the MachineCommand whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerMachineCommand | Remove-BrokerMachineCommandMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the MachineCommand in the site

Remove-BrokerMachineConfiguration

Sep 10, 2014

Deletes a machine configuration from the site or removes the association from a desktop group.

Syntax

```
Remove-BrokerMachineConfiguration [-InputObject] <MachineConfiguration[]> [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerMachineConfiguration [-Name] <String> [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-MachineConfiguration cmdlet deletes machine configurations from the site. A machine configuration cannot be removed while it is applied to a desktop group.

When a desktop group is provided, the Remove-MachineConfiguration cmdlet removes the association between machine configuration and the desktop group. In this case, the machine configuration is not removed from the site.

Related topics

New-BrokerMachineConfiguration

Get-BrokerMachineConfiguration

Set-BrokerMachineConfiguration

Rename-BrokerMachineConfiguration

Add-BrokerMachineConfiguration

Parameters

-InputObject<MachineConfiguration[]>

Machine configuration to remove.

Required?	true
Default Value	None
Accept Pipeline Input?	true (ByValue)

-Name<String>

Name of machine configuration for which the remove operation applies.

Required?	true

Default Value	None
Accept Pipeline Input?	true (ByPropertyName)

-DesktopGroup<DesktopGroup>

The desktop group from which this machine configuration is to be removed.

Required?	false
Default Value	None
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.MachineConfiguration Machine configuration to remove

Return Values

None

Notes

A machine configuration can only be removed if it is not currently applied to a desktop group.

Examples

---------- EXAMPLE 1 ----------

```
Remove-BrokerMachineConfiguration -Name UPM\Finance
```

Removes the machine configuration named "UPM\Finance".

---------- EXAMPLE 2 ----------

```
Remove-BrokerMachineConfiguration -Name Receiver\HumanResources -DesktopGroup SharedWorkers
```

Removes the association of the machine configuration named "Receiver\HumanResources" from the "SharedWorkers" desktop group.

Remove-BrokerMachineConfigurationMetadata

Sep 10, 2014

Deletes MachineConfiguration Metadata from the MachineConfiguration objects

Syntax

Remove-BrokerMachineConfigurationMetadata [-InputObject] <MachineConfiguration[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerMachineConfigurationMetadata cmdlet deletes Metadata from the MachineConfiguration objects.

Related topics

Parameters

-InputObject<MachineConfiguration[]>

Specifies the MachineConfiguration object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerMachineConfiguration You can pipe the MachineConfiguration to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerMachineConfigurationMetadata -InputObject $obj-Uid -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for the MachineConfiguration whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerMachineConfiguration | Remove-BrokerMachineConfigurationMetadata -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for all the MachineConfiguration in the site

Remove-BrokerMachineMetadata

Sep 10, 2014

Deletes Machine Metadata from the Machine objects

Syntax

Remove-BrokerMachineMetadata [-InputObject] <Machine[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerMachineMetadata cmdlet deletes Metadata from the Machine objects.

Related topics

Parameters

-InputObject<Machine[]>

Specifies the Machine object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerMachine You can pipe the Machine to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerMachineMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the Machine whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerMachine | Remove-BrokerMachineMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the Machine in the site

Remove-BrokerPowerTimeScheme

Sep 10, 2014

Deletes an existing power time scheme.

Syntax

```
Remove-BrokerPowerTimeScheme [-InputObject] <PowerTimeScheme[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerPowerTimeScheme [-Name] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerPowerTimeScheme cmdlet deletes a power time scheme from the system, and leaves the days that the time scheme used to cover for the associated desktop group as defaulting to all hours off-peak and all hours with pool size of -1.

Each power time scheme is associated with a particular desktop group, and covers one or more days of the week, defining which hours of those days are considered peak times and which are off-peak times. In addition, the time scheme defines a pool size value for each hour of the day for the days of the week covered by the time scheme. No one desktop group can be associated with two or more time schemes that cover the same day of the week.

For more information about the power policy mechanism and pool size management, see 'help about_Broker_PowerManagement'.

Related topics

Get-BrokerPowerTimeScheme

Set-BrokerPowerTimeScheme

New-BrokerPowerTimeScheme

Rename-BrokerPowerTimeScheme

Parameters

-InputObject<PowerTimeScheme[]>

The power time scheme to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the power time scheme to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.PowerTimeScheme The power time scheme to be deleted.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerPowerTimeScheme -Name 'Development Weekdays'
```

Deletes the power time scheme named 'Development Weekdays'.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerPowerTimeScheme -DesktopGroupUid (Get-BrokerDesktopGroup -name 'Finance desk1').Uid  | Remove-BrokerPowerTimeScheme
```

Deletes all power time schemes for the desktop group named 'Finance desk1'.

Remove-BrokerPowerTimeSchemeMetadata

Sep 10, 2014

Deletes PowerTimeScheme Metadata from the PowerTimeScheme objects

Syntax

```
Remove-BrokerPowerTimeSchemeMetadata [-InputObject] <PowerTimeScheme[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerPowerTimeSchemeMetadata cmdlet deletes Metadata from the PowerTimeScheme objects.

Related topics

Parameters

-InputObject<PowerTimeScheme[]>

Specifies the PowerTimeScheme object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerPowerTimeScheme You can pipe the PowerTimeScheme to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerPowerTimeSchemeMetadata -InputObject $obj-Uid -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for the PowerTimeScheme whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerPowerTimeScheme | Remove-BrokerPowerTimeSchemeMetadata -Name "MyMetadataName"
This command deletes the Metadata "MyMetadataName" key-value pair for all the PowerTimeScheme in the site

Remove-BrokerRebootCycleMetadata

Sep 10, 2014

Deletes RebootCycle Metadata from the RebootCycle objects

Syntax

Remove-BrokerRebootCycleMetadata [-InputObject] <RebootCycle[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerRebootCycleMetadata cmdlet deletes Metadata from the RebootCycle objects.

Related topics

Parameters

-InputObject<RebootCycle[]>

Specifies the RebootCycle object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerRebootCycle You can pipe the RebootCycle to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerRebootCycleMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the RebootCycle whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerRebootCycle | Remove-BrokerRebootCycleMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the RebootCycle in the site

Remove-BrokerRebootSchedule

Sep 10, 2014

Removes the reboot schedule.

Syntax

Remove-BrokerRebootSchedule [-InputObject] <RebootSchedule[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerRebootSchedule [-DesktopGroupName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerRebootSchedule cmdlet is used to delete an existing reboot schedule.

Related topics

Get-BrokerRebootSchedule

Set-BrokerRebootSchedule

New-BrokerRebootSchedule

Stop-BrokerRebootCycle

Parameters

-InputObject<RebootSchedule[]>

The reboot schedule to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroupName<String>

The name of the desktop group whose reboot schedule is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.RebootSchedule Reboot schedules may be specified through pipeline input.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerRebootSchedule | Remove-BrokerRebootSchedule
```

Deletes every reboot schedule.

---------- EXAMPLE 2 ----------

```
C:\PS> Remove-BrokerRebootSchedule 12
```

Deletes the reboot schedule for the desktop group having Uid 12.

---------- EXAMPLE 3 ----------

```
C:\PS> Remove-BrokerRebootSchedule -DesktopGroupName Accounting
```

Deletes the reboot schedule for the desktop group named Accounting.

Remove-BrokerRemotePCAccount

Sep 10, 2014

Delete RemotePCAccounts from the system.

Syntax

```
Remove-BrokerRemotePCAccount [-InputObject] <RemotePCAccount[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Delete RemotePCAccounts from the site.

Related topics

Get-BrokerRemotePCAccount

New-BrokerRemotePCAccount

Set-BrokerRemotePCAccount

Parameters

-InputObject<RemotePCAccount[]>

Specifies the RemotePCAccounts to delete.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.RemotePCAccount You can pipe the RemotePCAccounts to be deleted into this cmdlet.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-BrokerRemotePCAccount 42
Delete RemotePCAccount 42.

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerRemotePCAccount -OU 'any' | Remove-BrokerRemotePCAccount
Delete the 'any' OU RemotePCAccount.

---------- EXAMPLE 3 ----------

C:\PS> Get-BrokerRemotePCAccount | Remove-BrokerRemotePCAccount
Delete all RemotePCAccounts.

Remove-BrokerScope

Sep 10, 2014

Remove the specified catalog/desktop group from the given scope(s).

Syntax

```
Remove-BrokerScope [-InputObject] <Scope[]> [-Catalog <Catalog>] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerScope cmdlet is used to remove a catalog/desktop group object from the given scope(s).

To remove a catalog/desktop group from a scope you need permission to change the scopes of the catalog/desktop group.

If the catalog/desktop group is not in a specified scope, that scope will be silently ignored.

Related topics

Parameters

-InputObject<Scope[]>

Specifies the scopes to remove the object from.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByValue)

-Catalog<Catalog>

Specifies the catalog object to be removed.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroup<DesktopGroup>

Specifies the desktop group object to be removed.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Scope You can pipe scopes to Remove-BrokerScope.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerScope -Scope Chalfont,Cambourne -DesktopGroup "Win7 Desktops"
```

Removes the "Win7 Desktops" desktop group from both the Chalfont and Cambourne scopes.

---------- EXAMPLE 2 ----------

```
C:\PS> 'Chalfont','Cambourne' | Remove-BrokerScope -DesktopGroup 'Win7 Desktops'
```

Removes the "Win7 Desktops" desktop group from both the Chalfont and Cambourne scopes.

Remove-BrokerSessionLinger

Sep 10, 2014

Removes a session linger setting.

Syntax

```
Remove-BrokerSessionLinger [-InputObject] <SessionLinger[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerSessionLinger [-DesktopGroupName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerSessionLinger cmdlet is used to delete an existing session linger setting.

Related topics

New-BrokerSessionLinger

Get-BrokerSessionLinger

Set-BrokerSessionLinger

Parameters

-InputObject<SessionLinger[]>

The session linger setting to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroupName<String>

The name of the desktop group whose session linger setting is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.SessionLinger Session linger settings may be specified through pipeline input.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerSessionLinger | Remove-BrokerSessionLinger
```

Deletes every session linger setting for all desktop groups.

Remove-BrokerSessionMetadata

Sep 10, 2014

Deletes Session Metadata from the Session objects

Syntax

Remove-BrokerSessionMetadata [-InputObject] <Session[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerSessionMetadata cmdlet deletes Metadata from the Session objects.

Related topics

Parameters

-InputObject<Session[]>

Specifies the Session object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerSession You can pipe the Session to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerSessionMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the Session whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerSession | Remove-BrokerSessionMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the Session in the site

Remove-BrokerSessionPreLaunch

Sep 10, 2014

Removes a session pre-launch setting.

Syntax

```
Remove-BrokerSessionPreLaunch [-InputObject] <SessionPreLaunch[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerSessionPreLaunch [-DesktopGroupName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerSessionPreLaunch cmdlet is used to delete an existing session pre-launch setting.

Related topics

New-BrokerSessionPreLaunch

Get-BrokerSessionPreLaunch

Set-BrokerSessionPreLaunch

Parameters

-InputObject<SessionPreLaunch[]>

The session pre-launch setting to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroupName<String>

The name of the desktop group whose session pre-launch setting is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.SessionPreLaunch Session pre-launch settings may be specified through pipeline input.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerSessionPreLaunch | Remove-BrokerSessionPreLaunch
```

Deletes every session pre-launch setting for all desktop groups.

Remove-BrokerSiteMetadata

Sep 10, 2014

Deletes Site Metadata from the Site objects

Syntax

Remove-BrokerSiteMetadata -Name <String> [[-InputObject] <Site[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerSiteMetadata cmdlet deletes Metadata from the Site objects.

Related topics

Parameters

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-InputObject<Site[]>

Specifies the Site object's instance whose Metadata is to be deleted.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerSite You can pipe the Site to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerSiteMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the Site

Remove-BrokerTag

Sep 10, 2014

Removes a tag from the system or clears a tag to object association.

Syntax

Remove-BrokerTag [-InputObject] <Tag[]> [-Desktop <Desktop>] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-BrokerTag [-Name] <String> [-Desktop <Desktop>] [-DesktopGroup <DesktopGroup>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Clears tag to object associations or delete tags from the system altogether.

To clear an association, supply one of the Application, DesktopGroup or PrivateDesktop parameters.

To delete the tag, and any associations between the tag and other objects in the database, specify the tag without any associated object parameters.

Related topics

Add-BrokerTag

Get-BrokerTag

New-BrokerTag

Rename-BrokerTag

Parameters

-InputObject<Tag[]>

Specifies one or more tag objects.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies a tag by name.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Desktop<Desktop>

Clears the association between the given tag and Desktop.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroup<DesktopGroup>

Clears the association between the given tag and desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Tag Tags may be specified through pipeline input.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerTag $tag -Desktop $desktop
```

Clears the association between a tag and a desktop. Note that the tag itself continues to exist as an object in the database.

---------- EXAMPLE 2 ----------

```
C:\PS> Remove-BrokerTag $tag
```

Deletes the tag object from the database and clears any associations that may exist between that tag and other objects.

Remove-BrokerTagMetadata

Sep 10, 2014

Deletes Tag Metadata from the Tag objects

Syntax

Remove-BrokerTagMetadata [-InputObject] <Tag[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-BrokerTagMetadata cmdlet deletes Metadata from the Tag objects.

Related topics

Parameters

-InputObject<Tag[]>

Specifies the Tag object's instance whose Metadata is to be deleted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata to be deleted

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerTag You can pipe the Tag to delete the metadata.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-BrokerTagMetadata -InputObject $obj-Uid -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for the Tag whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerTag | Remove-BrokerTagMetadata -Name "MyMetadataName"
```

This command deletes the Metadata "MyMetadataName" key-value pair for all the Tag in the site

Remove-BrokerUser

Sep 10, 2014

Remove broker user objects from another broker object

Syntax

```
Remove-BrokerUser [-InputObject] <User[]> [-Application <Application>] [-SessionLinger <SessionLinger>] [-SessionPreLaunch <SessionPreLaunch>] [-Machine <Machine>] [-PrivateDesktop <PrivateDesktop>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Remove-BrokerUser [-Name] <String> [-Application <Application>] [-SessionLinger <SessionLinger>] [-SessionPreLaunch <SessionPreLaunch>] [-Machine <Machine>] [-PrivateDesktop <PrivateDesktop>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-BrokerUser cmdlet removes broker user objects from another specified object, such as a broker private desktop, to which the user had previously been added.

Related topics

Add-BrokerUser

Get-BrokerUser

Parameters

-InputObject<User[]>

Specifies the user objects to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the user objects to remove, based on their Name property.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-Application<Application>

The application from which to remove the user

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByValue)

-SessionLinger<SessionLinger>

The desktop group session linger setting from which to remove the user.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByValue)

-SessionPreLaunch<SessionPreLaunch>

The desktop group session pre-launch setting from which to remove the user.

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByValue)

-Machine<Machine>

The machine from which to remove the user

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByValue)

-PrivateDesktop<PrivateDesktop>

The desktop from which to remove the user

Required?	false
Default Value	null
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.USer You can pipe the users to be removed to Remove-BrokerUser.

Return Values

None

Notes

Specify one of the -Machine or -PrivateDesktop parameters only.

Examples

---------- EXAMPLE 1 ----------

```
Remove-BrokerUser "DOMAIN\UserName" -PrivateDesktop "DOMAIN\MachineName"
```

Remove the assignment of the specified private desktop to the specified user.

Rename-BrokerAccessPolicyRule

Sep 10, 2014

Renames a rule in the site's access policy.

Syntax

```
Rename-BrokerAccessPolicyRule [-InputObject] <AccessPolicyRule[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerAccessPolicyRule [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-BrokerAccessPolicyRule cmdlet renames a rule in the site's access policy. The Name property of the rule is changed.

An access policy rule defines a set of connection filters and access control rights relating to a desktop group. These allow fine-grained control of what access is granted to a desktop group based on details of, for example, a user's endpoint device, its address, and the user's identity.

Related topics

New-BrokerAccessPolicyRule

Get-BrokerAccessPolicyRule

Set-BrokerAccessPolicyRule

Remove-BrokerAccessPolicyRule

Parameters

-InputObject<AccessPolicyRule[]>

The access policy rule to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The existing name of the access policy rule to be renamed.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

The new name for the access policy rule being renamed. The new name must not match that of any other existing rules in the policy.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host

name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AccessPolicyRule The access policy rule to be renamed.

Return Values

None or Citrix.Broker.Admin.SDK.AccessPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AccessPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-BrokerAccessPolicyRule 'Sales' -NewName 'TeleSales'
```

Renames the access policy rule called Sales to TeleSales. The new name of the rule must be unique in the access policy.

Rename-BrokerAdminFolder

Sep 10, 2014

Renames a folder

Syntax

Rename-BrokerAdminFolder [-InputObject] <AdminFolder[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerAdminFolder [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Rename-BrokerAdminFolder cmdlet renames a folder for organising objects for administration purposes (for example, Applications).

The following special characters are not allowed in the new FolderName: \ / ; : # . * ? = < > | [ ] ( ) " ' `

Related topics

Get-BrokerAdminFolder

New-BrokerAdminFolder

Parameters

-InputObject<AdminFolder[]>

The folder(s) to be renamed

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

A pattern matching the names of folders to be renamed

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

The name the new folder(s) should have.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.

Accept Pipeline Input?	false

Input Type

Depends on parameter Parameters can be piped by property name.

Return Values

None or Citrix.Broker.Admin.SDK.AdminFolder

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AdminFolder object.

Examples

---------- EXAMPLE 1 ----------

```
Rename-BrokerAdminFolder F1\XXX\ YYY
```

Renames the folder called XXX within the folder F1\ to YYY

Rename-BrokerAppAssignmentPolicyRule

Sep 10, 2014

Renames an application rule in the site's assignment policy.

Syntax

```
Rename-BrokerAppAssignmentPolicyRule [-InputObject] <AppAssignmentPolicyRule[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerAppAssignmentPolicyRule [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-BrokerAppAssignmentPolicyRule cmdlet renames an application rule in the site's assignment policy. The Name property of the rule is changed.

An application rule in the assignment policy defines the users who are entitled to a self-service persistent machine assignment from the rule's desktop group; once assigned the machine can run one or more applications published from the group.

Related topics

New-BrokerAppAssignmentPolicyRule

Get-BrokerAppAssignmentPolicyRule

Set-BrokerAppAssignmentPolicyRule

Remove-BrokerAppAssignmentPolicyRule

Parameters

-InputObject<AppAssignmentPolicyRule[]>

The application rule in the assignment policy to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The existing name of the application rule in the assignment policy to be renamed.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

The new name of the application rule in the assignment policy being renamed. The new name must not match that of any other existing rule in the policy (irrespective of whether it is a desktop or application rule).

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host

name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AppAssignmentPolicyRule The application rule in the assignment policy being renamed.

Return Values

None or Citrix.Broker.Admin.SDK.AppAssignmentPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AppAssignmentPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-BrokerAppAssignmentPolicyRule 'Offshore' -NewName 'Remote Workers'
```

Renames the application rule in the assignment policy called Offshore to Remote Workers. The new name of the rule must be unique in the assignment policy.

Rename-BrokerAppEntitlementPolicyRule

Sep 10, 2014

Renames an application rule in the site's entitlement policy.

Syntax

```
Rename-BrokerAppEntitlementPolicyRule [-InputObject] <AppEntitlementPolicyRule[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Rename-BrokerAppEntitlementPolicyRule [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-BrokerAppEntitlementPolicyRule cmdlet renames an application rule in the site's entitlement policy. The Name property of the rule is changed.

An application rule in the entitlement policy defines the users who are allowed per-session access to a machine to run one or more applications published from the rule's desktop group.

Related topics

New-BrokerAppEntitlementPolicyRule

Get-BrokerAppEntitlementPolicyRule

Set-BrokerAppEntitlementPolicyRule

Remove-BrokerAppEntitlementPolicyRule

Parameters

-InputObject<AppEntitlementPolicyRule[]>

The application rule in the entitlement policy to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The existing name of the application rule in the entitlement policy to be renamed.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

The new name of the application rule in the entitlement policy being renamed. The new name must not match that of any other existing rule in the policy (irrespective of whether it is a desktop or application rule).

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AppEntitlementPolicyRule The application rule in the entitlement policy being renamed.

Return Values

None or Citrix.Broker.Admin.SDK.AppEntitlementPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AppEntitlementPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-BrokerAppEntitlementPolicyRule 'Prod Dev' -NewName 'Product Development'
```

Renames the application rule in the entitlement policy called Prod Dev to Product Development. The new name of the rule must be unique in the entitlement policy.

Rename-BrokerApplication

Sep 10, 2014

Renames an application.

Syntax

```
Rename-BrokerApplication [-InputObject] <Application[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerApplication [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-BrokerApplication cmdlet changes the administrative name of an application. An application cannot have the same name as another application.

Renaming an application does not alter its published name. To change the name with which this application appears to end-users, set a new value for the PublishedName property using the Set-BrokerApplication cmdlet.

Renaming an application does not alter its BrowserName. If the BrowserName property also needs to be changed, use the Set-BrokerApplication cmdlet to modify it.

Related topics

New-BrokerApplication

Set-BrokerApplication

Get-BrokerApplication

Remove-BrokerApplication

Parameters

-InputObject<Application[]>

Specifies the application to rename.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the application to rename.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

Specifies the new name for the application.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host

name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Application You can pipe applications to Rename-BrokerApplication.

Return Values

None or Citrix.Broker.Admin.SDK.Application

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.Application object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-BrokerApplication -Name "Old Name" -NewName "New Name"
```

Renames the application with name "Old Name" to "New Name".

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerApplication -Uid 1 | Rename-BrokerApplication -NewName "New Name" -PassThru
```

Renames application with the Uid 1 to "New Name", showing the result.

Rename-BrokerAssignmentPolicyRule

Sep 10, 2014

Renames a desktop rule in the site's assignment policy.

Syntax

```
Rename-BrokerAssignmentPolicyRule [-InputObject] <AssignmentPolicyRule[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerAssignmentPolicyRule [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-BrokerAssignmentPolicyRule cmdlet renames a desktop rule in the site's assignment policy. The Name property of the rule is changed.

A desktop rule in the assignment policy defines the users who are entitled to self-service persistent machine assignments from the rule's desktop group. A rule defines how many machines a user is allowed from the group for delivery of full desktop sessions.

Related topics

New-BrokerAssignmentPolicyRule

Get-BrokerAssignmentPolicyRule

Set-BrokerAssignmentPolicyRule

Remove-BrokerAssignmentPolicyRule

Parameters

-InputObject<AssignmentPolicyRule[]>

The desktop rule in the assignment policy to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The existing name of the desktop rule in the assignment policy to be renamed.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

The new name of the desktop rule in the assignment policy being renamed. The new name must not match that of any other existing rule in the policy (irrespective of whether it is a desktop or application rule).

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host

name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AssignmentPolicyRule The desktop rule in the assignment policy being renamed.

Return Values

None, or Citrix.Broker.Admin.SDK.AssignmentPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AssignmentPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-BrokerAssignmentPolicyRule 'Offshore' -NewName 'Remote Workers'
```

Renames the desktop rule in the assignment policy called Offshore to Remote Workers. The new name of the rule must be unique in the assignment policy.

Rename-BrokerCatalog

Sep 10, 2014

Renames a catalog.

Syntax

```
Rename-BrokerCatalog [-InputObject] <Catalog[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerCatalog [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-BrokerCatalog cmdlet changes the name of a catalog. A catalog cannot have the same name as another catalog.

The following special characters are not allowed in a catalog name: \ / ; : # . * ? = < > | [ ] ( ) " ' `

Related topics

Get-BrokerCatalog

New-BrokerCatalog

Remove-BrokerCatalog

Set-BrokerCatalog

Parameters

-InputObject<Catalog[]>

Specifies the catalog to rename.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the catalog to rename.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

Specifies the new name of the catalog.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Catalog You can pipe catalogs to Rename-BrokerCatalog.

Return Values

None or Citrix.Broker.Admin.SDK.Catalog

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.Catalog object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-BrokerCatalog -Name "Old Name" -NewName "New Name"
```

Renames the catalog with the name "Old Name" to "New Name".

---------- EXAMPLE 2 ----------

```
C:\PS> c:\$catalog = Get-BrokerCatalog -Name "Old Name"
C:\PS> Rename-BrokerCatalog -InputObject $catalog -NewName "New Name"
```

Renames the catalog with the name "Old Name" to "New Name".

Rename-BrokerDesktopGroup

Sep 10, 2014

Renames a desktop group.

Syntax

```
Rename-BrokerDesktopGroup [-InputObject] <DesktopGroup[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerDesktopGroup [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-BrokerDesktopGroup cmdlet changes the name of a desktop group. A desktop group cannot have the same name as another desktop group.

Related topics

Get-BrokerDesktopGroup

New-BrokerDesktopGroup

Set-BrokerDesktopGroup

Remove-BrokerDesktopGroup

Parameters

-InputObject<DesktopGroup[]>

Specifies the desktop group to rename.

Required?	true
Default Value	null
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the desktop group to rename.

Required?	true
Default Value	null

Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

Specifies the new name that the desktop group will have.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.DesktopGroup You can pipe desktop groups to Rename-BrokerDesktopGroup.

Return Values

None or Citrix.Broker.Admin.SDK.DesktopGroup

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.DesktopGroup object.

Notes

Renaming a desktop group does not alter its published name. If you need to change the name with which this desktop group appears to end-users, set a new value for the PublishedName property using the Set-BrokerDesktopGroup cmdlet.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-BrokerDesktopGroup -Name "Old Name" -NewName "New Name"
```

Renames desktop group with the name "Old Name" to "New Name".

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerDesktopGroup -Uid 1 | Rename-BrokerDesktopGroup -NewName "New Name" -PassThru
```

Renames desktop group with the Uid 1 to "New Name", showing the result.

Rename-BrokerEntitlementPolicyRule

Sep 10, 2014

Renames a desktop rule in the site's entitlement policy.

Syntax

```
Rename-BrokerEntitlementPolicyRule [-InputObject] <EntitlementPolicyRule[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Rename-BrokerEntitlementPolicyRule [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-BrokerEntitlementPolicyRule cmdlet renames a desktop rule in the site's entitlement policy. The Name property of the rule is changed.

A desktop rule in the entitlement policy defines the users who are allowed per-session access to a machine from the rule's associated desktop group to run a full desktop session.

Related topics

New-BrokerEntitlementPolicyRule

Get-BrokerEntitlementPolicyRule

Set-BrokerEntitlementPolicyRule

Remove-BrokerEntitlementPolicyRule

Parameters

-InputObject<EntitlementPolicyRule[]>

The desktop rule in the entitlement policy to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The existing name of the desktop rule in the entitlement policy to be renamed.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

The new name of the desktop rule in the entitlement policy being renamed. The new name must not match that of any other existing rule in the policy (irrespective of whether it is a desktop or application rule).

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.EntitlementPolicyRule The desktop rule in the entitlement policy being renamed.

Return Values

None or Citrix.Broker.Admin.SDK.EntitlementPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.EntitlementPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-BrokerEntitlementPolicyRule 'Prod Dev' -NewName 'Product Development'
```

Renames the desktop rule in the entitlement policy called Prod Dev to Product Development. The new name of the rule must be unique in the entitlement policy.

Rename-BrokerMachineConfiguration

Sep 10, 2014

Renames a machine configuration.

Syntax

Rename-BrokerMachineConfiguration [-InputObject] <MachineConfiguration[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerMachineConfiguration [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Rename-MachineConfiguration cmdlet changes the name of a machine configuration. A machine configuration cannot have the same name as another machine configuration associated with the same slot.

Related topics

New-BrokerMachineConfiguration

Get-BrokerMachineConfiguration

Set-BrokerMachineConfiguration

Remove-BrokerMachineConfiguration

Add-BrokerMachineConfiguration

Parameters

-InputObject<MachineConfiguration[]>

Machine configuration to rename.

Required?	true
Default Value	None
Accept Pipeline Input?	true (ByValue)

-Name<String>

Current name of machine configuration.

Required?	true
Default Value	None

Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

New name for machine configuration. This may have the form "ConfigurationSlotName\MachineConfigurationName" or "MachineConfigurationName". If the "ConfigurationSlotName" is provided it must match the name of the configuration slot that the machine configuration is associated with.

Required?	true
Default Value	None
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.MachineConfiguration Machine configuration to rename.

Return Values

None or Citrix.Broker.Admin.SDK.MachineConfiguration

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.MachineConfiguration object.

Notes

The configuration slot can not be changed. Thus the left term of the Name and NewName must match.

Examples

---------- EXAMPLE 1 ----------

Rename-BrokerMachineConfiguration -Name "UPM\All Departments" -NewName "UPM\Finance Department"
Renames the machine configuration named "UPM\All Departments" to "UPM\Finance Department".

---------- EXAMPLE 2 ----------

Rename-BrokerMachineConfiguration -Name "UPM\All Departments" -NewName "Finance Department"
Renames the machine configuration named "UPM\All Departments" to "UPM\Finance Department".

Rename-BrokerPowerTimeScheme

Sep 10, 2014

Changes the name of an existing power time scheme.

Syntax

```
Rename-BrokerPowerTimeScheme [-InputObject] <PowerTimeScheme[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerPowerTimeScheme [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-BrokerPowerTimeScheme cmdlet renames a particular power time scheme.

Each power time scheme is associated with a particular desktop group, and covers one or more days of the week, defining which hours of those days are considered peak times and which are off-peak times. In addition, the time scheme defines a pool size value for each hour of the day for the days of the week covered by the time scheme. No one desktop group can be associated with two or more time schemes that cover the same day of the week.

For more information about the power policy mechanism and pool size management, see 'help about_Broker_PowerManagement'.

Related topics

Get-BrokerPowerTimeScheme

Set-BrokerPowerTimeScheme

New-BrokerPowerTimeScheme

Remove-BrokerPowerTimeScheme

Parameters

-InputObject<PowerTimeScheme[]>

The power time scheme to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The current name of the power time scheme to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

The new name to be applied to the power time scheme.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.PowerTimeScheme The power time scheme to be renamed.

Return Values

None or Citrix.Broker.Admin.SDK.PowerTimeScheme

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.PowerTimeScheme object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Rename-BrokerPowerTimeScheme -Name 'Development Weekdays' -NewName 'Dev Week'
Renames the power time scheme named 'Development Weekdays' to 'Dev Week'.

Rename-BrokerTag

Sep 10, 2014

Rename one or more tags.

Syntax

```
Rename-BrokerTag [-InputObject] <Tag[]> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-BrokerTag [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Renames one or more tags with the supplied name.

Related topics

Add-BrokerTag

Get-BrokerTag

New-BrokerTag

Remove-BrokerTag

Parameters

-InputObject<Tag[]>

Specifies one or more tag objects to rename.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Identifies tags to be renamed by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

Specifies new name for the tags.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.

Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Tag The tag to rename can be piped into this cmdlet.

Return Values

None or Citrix.Broker.Admin.SDK.Tag

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.Tag object.

Notes

Note that when renaming a tag, its UUID remains the same and any associations are maintained.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-BrokerTag -Name 'OldName' -NewName 'ReplacementName'
```

Renames tags with the name 'OldName' to 'ReplacementName'.

Reset-BrokerLicensingConnection

Sep 10, 2014

Resets the broker's license server connection.

Syntax

```
Reset-BrokerLicensingConnection [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Reset-BrokerLicensingConnection cmdlet resets the broker's connection to the license server.

Licensing changes resulting from new license files or alterations to the site-level licensing properties don't become effective immediately. There will typically be a delay as the changes are propagated across the site based on the scheduling of refresh logic built into the controllers and the license server.

Resetting the connection causes the list of available licenses for the connection to be updated. After adding licenses or changing the site-level licensing properties you can run Reset-BrokerLicensingConnection to ensure that the broker can access the new licenses immediately.

Each broker service instance holds its own connection to the license server. In order for the licensing changes to be applied immediately throughout the XenDesktop site this command needs to be run on every controller in the site.

Related topics

Get-BrokerSite

Set-BrokerSite

Parameters

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Reset-BrokerLicensingConnection

Reset the broker's license server connection.

Reset-BrokerServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the Broker Service.

Syntax

```
Reset-BrokerServiceGroupMembership -ConfigServiceInstance <PSObject[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Enables you to reload Broker Service access permissions and configuration service locations. The Reset-BrokerServiceGroupMembership command must be run on at least one instance of the service type (Broker) after installation and registration with the configuration service. Without this operation, the Broker services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-BrokerServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Get-BrokerServiceInstance

Get-BrokerServiceStatus

Parameters

-ConfigServiceInstance<PSObject[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	LocalHost
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-BrokerServiceGroupMembership command.

Return Values

Citrix.Broker.Sdk.ServiceInstance

Reset-BrokerServiceGroupMembership returns opaque objects containing Configuration Service instances that are used by the Broker Service instance.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-BrokerServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-BrokerServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Send-BrokerSessionMessage

Sep 10, 2014

Sends a message to a session.

Syntax

Send-BrokerSessionMessage [-InputObject] <Session[]> [-MessageStyle] <SendMessageStyle> [-Title] <String> [-Text] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Generates a message box in the target session(s).

Related topics

Get-BrokerSession

Parameters

-InputObject<Session[]>

The target session(s) to send the message to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MessageStyle<SendMessageStyle>

The style of message box to use (valid values are Critical, Question, Exclamation, or Information).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Title<String>

Text to display in the messagebox title bar.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Text<String>

The message to display.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Session The session to which to send the message can be piped in.

Return Values

None

Notes

Sessions can be passed as the InputObject parameter as either session objects or their numeric Uids.

This operation is non-blocking and returns before it completes. The operation, however, is unlikely to fail unless there are communication problems between controller and machine, if bad arguments are passed to the cmdlet itself or if the machine cannot successfully execute the operation.

The transient nature of sessions means that the list of session objects or UIDs supplied to Send-BrokerSessionMessage could consist of valid and invalid sessions. Invalid sessions are detected and disregarded and the send message operation is invoked on the machines running valid sessions.

The system can fail to invoke the operation if the machine is not in an appropriate state or if there are problems in communicating with the machine. When an operation is invoked the system detects if the operation was initiated successfully or not by the session. As this operation is non-blocking the system doesn't detect or report whether the operation ultimately succeeded or failed after its successful initialization in the session.

Operation failures are reported through the broker SDK error handling mechanism (see about_Broker_ErrorHandling). In the event of errors the SdkErrorRecord error status code is set to SessionOperationFailed and its error data dictionary is populated with the following entries:

o OperationsAttemptedCount: The number of operations attempted.

o OperationsFailedCount - The number of failed operations.

o OperationsSucceededCount - The number of successfully executed operations.

o UnresolvedSessionFailuresCount - The number of operations that failed due to invalid sessions being supplied.

o OperationInvocationFailuresCount - The number of operations that failed because they could not be invoked in the session.

o DesktopExecutionFailuresCount - The number of operations that failed because they could not be successfully executed in the session.

The SdkErrorRecord message will also display the number of attempted, failed and successful operations in the following format:

"Session operation error - attempted:<OperationsAttemptedCount>, failed:<OperationsFailedCount>, succeeded:<OperationsSucceededCount>"

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $sessions = Get-BrokerSession -UserName MYDOMAIN\*
C:\PS> Send-BrokerSessionMessage $sessions -MessageStyle Information -Title TestTitle -Text TestMessage
```

Sends a message to all the sessions for any user in MYDOMAIN.

---------- EXAMPLE 2 ----------

```
C:\PS> $desktop = Get-BrokerDesktop -Uid 1
C:\PS> Send-BrokerSessionMessage $desktop.SessionUid -MessageStyle Information -Title TestTitle -Text TestMessage
```

Sends a message to the session on the desktop with Uid 1.

---------- EXAMPLE 3 ----------

```
C:\PS> trap  [Citrix.Broker.Admin.SDK.SdkOperationException]
C:\PS> {
C:\PS>   write $("Exception name = " + $_.Exception.GetType().FullName)
C:\PS>   write $("SdkOperationException.Status = " + $_.Exception.Status)
C:\PS>   write $("SdkOperationException.ErrorData=")
C:\PS>   $_.Exception.ErrorData
C:\PS>
C:\PS>   write $("SdkOperationException.InnerException = " + $_.Exception.InnerException)
C:\PS>   $_.Exception.InnerException
C:\PS>   continue
C:\PS> }
C:\PS>
C:\PS> Send-BrokerSessionMessage -InputObject 10,11,12 -MessageStyle Information -Title "message title" -Text "message text"
```

Trap and display error information.

Set-BrokerAccessPolicyRule

Sep 10, 2014

Modifies an existing rule in the site's access policy.

Syntax

Set-BrokerAccessPolicyRule [-InputObject] <AccessPolicyRule[]> [-PassThru] [-AddExcludedClientIPs <IPAddressRange[]>] [-AddExcludedClientNames <String[]>] [-AddExcludedSmartAccessTags <String[]>] [-AddExcludedUsers <User[]>] [-AddIncludedClientIPs <IPAddressRange[]>] [-AddIncludedClientNames <String[]>] [-AddIncludedSmartAccessTags <String[]>] [-AddIncludedUsers <User[]>] [-AllowedConnections <AllowedConnection>] [-AllowedProtocols <String[]>] [-AllowedUsers <AllowedUser>] [-AllowRestart <Boolean>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedClientIPFilterEnabled <Boolean>] [-ExcludedClientIPs <IPAddressRange[]>] [-ExcludedClientNameFilterEnabled <Boolean>] [-ExcludedClientNames <String[]>] [-ExcludedSmartAccessFilterEnabled <Boolean>] [-ExcludedSmartAccessTags <String[]>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-HdxSslEnabled <Boolean>] [-IncludedClientIPFilterEnabled <Boolean>] [-IncludedClientIPs <IPAddressRange[]>] [-IncludedClientNameFilterEnabled <Boolean>] [-IncludedClientNames <String[]>] [-IncludedSmartAccessFilterEnabled <Boolean>] [-IncludedSmartAccessTags <String[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-RemoveExcludedClientIPs <IPAddressRange[]>] [-RemoveExcludedClientNames <String[]>] [-RemoveExcludedSmartAccessTags <String[]>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedClientIPs <IPAddressRange[]>] [-RemoveIncludedClientNames <String[]>] [-RemoveIncludedSmartAccessTags <String[]>] [-RemoveIncludedUsers <User[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAccessPolicyRule [-Name] <String> [-PassThru] [-AddExcludedClientIPs <IPAddressRange[]>] [-AddExcludedClientNames <String[]>] [-AddExcludedSmartAccessTags <String[]>] [-AddExcludedUsers <User[]>] [-AddIncludedClientIPs <IPAddressRange[]>] [-AddIncludedClientNames <String[]>] [-AddIncludedSmartAccessTags <String[]>] [-AddIncludedUsers <User[]>] [-AllowedConnections <AllowedConnection>] [-AllowedProtocols <String[]>] [-AllowedUsers <AllowedUser>] [-AllowRestart <Boolean>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedClientIPFilterEnabled <Boolean>] [-ExcludedClientIPs <IPAddressRange[]>] [-ExcludedClientNameFilterEnabled <Boolean>] [-ExcludedClientNames <String[]>] [-ExcludedSmartAccessFilterEnabled <Boolean>] [-ExcludedSmartAccessTags <String[]>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-HdxSslEnabled <Boolean>] [-IncludedClientIPFilterEnabled <Boolean>] [-IncludedClientIPs <IPAddressRange[]>] [-IncludedClientNameFilterEnabled <Boolean>] [-IncludedClientNames <String[]>] [-IncludedSmartAccessFilterEnabled <Boolean>] [-IncludedSmartAccessTags <String[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-RemoveExcludedClientIPs <IPAddressRange[]>] [-RemoveExcludedClientNames <String[]>] [-RemoveExcludedSmartAccessTags <String[]>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedClientIPs <IPAddressRange[]>] [-RemoveIncludedClientNames <String[]>] [-RemoveIncludedSmartAccessTags <String[]>] [-RemoveIncludedUsers <User[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerAccessPolicyRule cmdlet modifies an existing rule in the site's access policy.

An access policy rule defines a set of connection filters and access control rights relating to a desktop group. These allow fine-grained control of what access is granted to a desktop group based on details of, for example, a user's endpoint device, its address, and the user's identity.

Changing a rule does not affect existing user sessions, but it may result in users being unable to launch new sessions, or reconnect to disconnected sessions if the change removes access to the desktop group delivering those sessions.

Related topics

New-BrokerAccessPolicyRule

Get-BrokerAccessPolicyRule

Rename-BrokerAccessPolicyRule

Remove-BrokerAccessPolicyRule

Parameters

-InputObject<AccessPolicyRule[]>

The access policy rule to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the access policy rule to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-AddExcludedClientIPs<IPAddressRange[]>

Adds the specified user device IP addresses to the excluded client IP address filter of the rule.

See the ExcludedClientIPs parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddExcludedClientNames<String[]>

Adds the specified user device names to the excluded client names filter of the rule.

See the ExcludedClientNames parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddExcludedSmartAccessTags<String[]>

Adds the specified SmartAccess tags to the excluded SmartAccess tags filter of the rule.

See the ExcludedSmartAccessTags parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddExcludedUsers<User[]>

Adds the specified users and groups to the excluded users filter of the rule.

See the ExcludedUsers parameter for more information.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AddIncludedClientIPs<IPAddressRange[]>

Adds the specified user device IP addresses to the included client IP address filter of the rule.

See the IncludedClientIPs parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddIncludedClientNames<String[]>

Adds the specified user device names to the included client names filter of the rule.

See the IncludedClientNames parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddIncludedSmartAccessTags<String[]>

Adds the specified SmartAccess tags to the included SmartAccess tags filter of the rule.

See the IncludedSmartAccessTags parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddIncludedUsers<User[]>

Adds the specified users and groups to the included users filter of the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AllowedConnections<AllowedConnection>

Changes whether connections must be local or via Access Gateway, and if so whether specified SmartAccess tags must be provided by Access Gateway with the connection. This property forms part of the included SmartAccess tags filter.

Valid values are Filtered, NotViaAG, and ViaAG.

For a detailed description of this property see "help about_Broker_AccessPolicy".

Required?	false

Default Value	
Accept Pipeline Input?	false

-AllowedProtocols<String[]>

Changes the protocols (for example HDX, RDP) available to the user for sessions delivered from the rule's desktop group. If the user gains access to a desktop group by multiple rules, the allowed protocol list is the combination of the protocol lists from all those rules.

If the protocol list is empty, access to the desktop group is implicitly denied.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AllowedUsers<AllowedUser>

Changes the behavior of the included users filter of the rule. This can restrict access to a list of named users or groups, allow access to any authenticated user, any user (whether authenticated or not), or only non-authenticated users. For a detailed description of this property see "help about_Broker_AccessPolicy".

Valid values are Filtered, AnyAuthenticated, Any, AnonymousOnly and FilteredOrAnonymous.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AllowRestart<Boolean>

Changes whether the user can restart sessions delivered from the rule's desktop group. Session restart is handled as follows: For sessions on single-session power-managed machines, the machine is powered off, and a new session launch request made; for sessions on multi-session machines, a logoff request is issued to the session, and a new session launch request made; otherwise the property is ignored.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Changes the description of the rule. The text is purely informational for the administrator, it is never visible to the end user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Changes whether the rule is enabled or disabled. A disabled rule is ignored when evaluating the site's access policy.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ExcludedClientIPFilterEnabled<Boolean>

Changes whether the excluded client IP address filter is enabled or disabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedClientIPs<IPAddressRange[]>

Changes the IP addresses of user devices explicitly denied access to the rule's desktop group. Addresses can be specified as simple numeric addresses or as subnet masks (for example, 10.40.37.5 or 10.40.0.0/16). This property forms part of the excluded client IP address filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedClientNameFilterEnabled<Boolean>

Changes whether the excluded client names filter is enabled or disabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedClientNames<String[]>

Changes which names of user devices are explicitly denied access to the rule's desktop group. This property forms part of the excluded client names filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedSmartAccessFilterEnabled<Boolean>

Changes whether the excluded SmartAccess tags filter is enabled or disabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedSmartAccessTags<String[]>

Changes which SmartAccess tags explicitly deny access to the rule's desktop group if any occur in those provided by Access Gateway with the user's connection. This property forms part of the excluded SmartAccess tags filter.

Required?	false

Default Value	
Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Changes whether the excluded users filter is enabled or disabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUsers<User[]>

Changes which users and groups are explicitly denied access to the rule's desktop group. This property forms part of the excluded users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HdxSslEnabled<Boolean>

Indicates whether SSL encryption is enabled for sessions delivered from the rule's desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedClientIPFilterEnabled<Boolean>

Changes whether the included client IP address filter is enabled or disabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedClientIPs<IPAddressRange[]>

Changes which IP addresses of user devices allowed access to the rule's desktop group. Addresses can be specified as simple numeric addresses or as subnet masks (for example, 10.40.37.5 or 10.40.0.0/16). This property forms part of the included client IP address filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedClientNameFilterEnabled<Boolean>

Changes whether the included client name filter is enabled or disabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedClientNames<String[]>

Changes which names of user devices are allowed access to the rule's desktop group. This property forms part of the included client names filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedSmartAccessFilterEnabled<Boolean>

Changes whether the included SmartAccess tags filter is enabled or disabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedSmartAccessTags<String[]>

Changes which SmartAccess tags grant access to the rule's desktop group if any occur in those provided by Access Gateway with the user's connection. This property forms part of the excluded SmartAccess tags filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Changes whether the included users filter is enabled or disabled. If the filter is disabled, it is ignored when the access policy rule is evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUsers<User[]>

Changes which users and groups are granted access to the rule's desktop group. This property forms part of the included users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveExcludedClientIPs<IPAddressRange[]>

Removes the specified user device IP addresses from the excluded client IP address filter of the rule.

See the ExcludedClientIPs parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveExcludedClientNames<String[]>

Removes the specified user device names from the excluded client names filter of the rule.

See the ExcludedClientNames parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveExcludedSmartAccessTags<String[]>

Removes the specified SmartAccess tags from the excluded SmartAccess tags filter of the rule.

See the ExcludedSmartAccessTags parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveExcludedUsers<User[]>

Removes the specified users and groups from the excluded users filter of the rule.

See the ExcludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveIncludedClientIPs<IPAddressRange[]>

Removes the specified user device IP addresses from the included client IP address filter of the rule.

See the IncludedClientIPs parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveIncludedClientNames<String[]>

Removes the specified client names from the included client names filter of the rule.

See the IncludedClientNames parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveIncludedSmartAccessTags<String[]>

Removes the specified SmartAccess tags from the included SmartAccess tags filter of the rule.

See the IncludedSmartAccessTags parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveIncludedUsers<User[]>

Removes the specified users and groups from the included users filter of the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AccessPolicyRule The access policy rule to be modified.

Return Values

None, or Citrix.Broker.Admin.SDK.AccessPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AccessPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerAccessPolicyRule 'Temp Staff' -AddIncludedUsers office\contractors
```

Adds user group OFFICE\contractors to the Temp Staff access policy rule. The resources that the group can access are dependent on the existing properties of the rule in addition to the site's assignment and entitlement policies.

---------- EXAMPLE 2 ----------

```
C:\PS> Set-BrokerAccessPolicyRule 'Temp Staff' -ExcludedClientIPFilterEnabled $true -AddExcludedClientIPs '10.15.0.0/16' -AllowedConnections ViaAG
```

Modifies the Temp Staff access policy rule to remove access to any user device with an IP address matching 10.15.0.0/16, and requires that all connections by the rule must come through Access Gateway (assuming that the included SmartAccess tags filter is enabled).

Set-BrokerAccessPolicyRuleMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for AccessPolicyRule

Syntax

Set-BrokerAccessPolicyRuleMetadata [-AccessPolicyRuleId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAccessPolicyRuleMetadata [-AccessPolicyRuleId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAccessPolicyRuleMetadata [-AccessPolicyRuleId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAccessPolicyRuleMetadata [-InputObject] <AccessPolicyRule[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAccessPolicyRuleMetadata [-InputObject] <AccessPolicyRule[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAccessPolicyRuleMetadata [-AccessPolicyRuleName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAccessPolicyRuleMetadata [-AccessPolicyRuleName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerAccessPolicyRuleMetadata cmdlet creates/updates metadata key-value pairs for AccessPolicyRule. The AccessPolicyRule can be specified by InputObject or piping.

Related topics

Parameters

-AccessPolicyRuleId<Int32>

Specifies the AccessPolicyRule object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<AccessPolicyRule[]>

Specifies the AccessPolicyRule objects whose Metadata is to be created/updated.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-AccessPolicyRuleName<String>

Specifies the AccessPolicyRule object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerAccessPolicyRule You can pipe the AccessPolicyRule to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerAccessPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerAccessPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerAccessPolicyRuleMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the AccessPolicyRule whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerAccessPolicyRule | Set-BrokerAccessPolicyRuleMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the AccessPolicyRule in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerAccessPolicyRuleMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the AccessPolicyRule in the site whose name is 'objname'

Set-BrokerAdminFolderMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for AdminFolder

Syntax

Set-BrokerAdminFolderMetadata [-AdminFolderId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAdminFolderMetadata [-AdminFolderId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAdminFolderMetadata [-AdminFolderId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAdminFolderMetadata [-InputObject] <AdminFolder[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAdminFolderMetadata [-InputObject] <AdminFolder[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAdminFolderMetadata [-AdminFolderName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAdminFolderMetadata [-AdminFolderName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerAdminFolderMetadata cmdlet creates/updates metadata key-value pairs for AdminFolder. The AdminFolder can be specified by InputObject or piping.

Related topics

Parameters

-AdminFolderId<Int32>

Specifies the AdminFolder object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<AdminFolder[]>

Specifies the AdminFolder objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminFolderName<String>

Specifies the AdminFolder object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerAdminFolder You can pipe the AdminFolder to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerAdminFolder

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerAdminFolder object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerAdminFolderMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the AdminFolder whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerAdminFolder | Set-BrokerAdminFolderMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the AdminFolder in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerAdminFolderMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the AdminFolder in the site whose name is 'objname'

Set-BrokerAppAssignmentPolicyRule

Sep 10, 2014

Modifies an existing application rule in the site's assignment policy.

Syntax

```
Set-BrokerAppAssignmentPolicyRule [-InputObject] <AppAssignmentPolicyRule[]> [-PassThru] [-AddExcludedUsers <User[]>] [-AddIncludedUsers <User[]>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedUsers <User[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAppAssignmentPolicyRule [-Name] <String> [-PassThru] [-AddExcludedUsers <User[]>] [-AddIncludedUsers <User[]>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedUsers <User[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Set-BrokerAppAssignmentPolicyRule cmdlet modifies an existing application rule in the site's assignment policy.

An application rule in the assignment policy defines the users who are entitled to a self-service persistent machine assignment from the rule's desktop group; once assigned the machine can run one or more applications published from the group.

Changing an application rule does not alter machine assignments that have already been made by the rule, nor does it affect active sessions to those machines in any way.

Related topics

New-BrokerAppAssignmentPolicyRule

Get-BrokerAppAssignmentPolicyRule

Rename-BrokerAppAssignmentPolicyRule

Remove-BrokerAppAssignmentPolicyRule

Parameters

-InputObject<AppAssignmentPolicyRule[]>

The application rule in the assignment policy to be modified.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the application rule in the assignment policy to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-AddExcludedUsers<User[]>

Adds the specified users to the excluded users filter of the application rule, that is, the users and groups who are explicitly denied an entitlement to a machine assignment from this rule.

See the ExcludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddIncludedUsers<User[]>

Adds the specified users to the included users filter of the application rule, that is, the users and groups who are granted an entitlement to a machine assignment by the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Changes the description of the application rule. The text is purely informational for the administrator, it is never visible to the end user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Enables or disables the application rule. A disabled rule is ignored when evaluating the site's assignment policy.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Enables or disables the excluded users filter. If the filter is disabled then any user entries in the filter are ignored when assignment policy rules are evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUsers<User[]>

Changes the excluded users filter of the application rule, that is, the users and groups who are explicitly denied an entitlement to a machine assignment from the rule.

This can be used to exclude users or groups who would otherwise gain access by groups specified in the included users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Enables or disables the included users filter. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to a machine assignment by the application rule.

Users who would be implicitly granted access when the filter is disabled can still be explicitly denied access using the excluded users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUsers<User[]>

Changes the included users filter of the application rule, that is, the users and groups who are granted an entitlement to a machine assignment by the rule.

If a user appears explicitly in the excluded users filter of the rule, or is a member of a group that appears in the excluded users filter, no entitlement is granted whether or not the user appears in the included users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveExcludedUsers<User[]>

Removes the specified users from the excluded users filter of the application rule, that is, the users and groups who are explicitly denied an entitlement to a machine assignment from this rule.

See the ExcludedUsers parameter for more information.

Required?	false

Default Value	
Accept Pipeline Input?	false

-RemoveIncludedUsers<User[]>

Removes the specified users from the included users filter of the application rule, that is, the users and groups who are granted an entitlement to a machine assignment by the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AppAssignmentPolicyRule The application rule within the assignment policy to be modified.

Return Values

None or Citrix.Broker.Admin.SDK.AppAssignmentPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AppAssignmentPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerAppAssignmentPolicyRule 'Temp Staff' -AddIncludedUsers office\interns
Adds the user group OFFICE\interns to the Temp Staff application rule in the assignment policy. This grants all members of that user group an entitlement to a machine in the rule's desktop group. The machines can run applications published from the group. The application session properties obtained using the rule are determined by the rule's other properties.

---------- EXAMPLE 2 ----------

C:\PS> Set-BrokerAppAssignmentPolicyRule 'Temp Staff' -Enabled $false
Disables the Temp Staff application rule in the assignment policy. This prevents further machine assignments being made using this rule until it is re-enabled. However, access to machines already assigned using the rule is not impacted.

Set-BrokerAppEntitlementPolicyRule

Sep 10, 2014

Modifies an existing application rule in the site's entitlement policy.

Syntax

Set-BrokerAppEntitlementPolicyRule [-InputObject] <AppEntitlementPolicyRule[]> [-PassThru] [-AddExcludedUsers <User[]>] [-AddIncludedUsers <User[]>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedUsers <User[]>] [-SessionReconnection <SessionReconnection>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAppEntitlementPolicyRule [-Name] <String> [-PassThru] [-AddExcludedUsers <User[]>] [-AddIncludedUsers <User[]>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedUsers <User[]>] [-SessionReconnection <SessionReconnection>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerAppEntitlementPolicyRule cmdlet modifies an existing application rule in the site's entitlement policy.

An application rule in the entitlement policy defines the users who are allowed per-session access to a machine to run one or more applications published from the rule's desktop group.

Changing a rule does not affect existing sessions launched using the rule, but if the change removes an entitlement to a machine that was previously granted, users may be unable to reconnect to a disconnected session on that machine.

Related topics

New-BrokerAppEntitlementPolicyRule

Get-BrokerAppEntitlementPolicyRule

Rename-BrokerAppEntitlementPolicyRule

Remove-BrokerAppEntitlementPolicyRule

Parameters

-InputObject<AppEntitlementPolicyRule[]>

The application rule in the entitlement policy to be modified.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the application rule in the entitlement policy to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-AddExcludedUsers<User[]>

Adds the specified users to the excluded users filter of the rule, that is, the users and groups who are explicitly denied entitlements to run applications published from the desktop group.

See the ExcludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddIncludedUsers<User[]>

Adds the specified users to the included users filter of the rule, that is, the users and groups who are granted an entitlement to an application session by the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Changes the description of the application rule. The text is purely informational for the administrator, it is never visible to the end user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Enables or disables the application rule. A disabled rule is ignored when evaluating the site's entitlement policy.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Enables or disables the excluded users filter. If the filter is disabled then any user entries in the filter are ignored when entitlement policy rules are evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUsers<User[]>

Changes the excluded users filter of the rule, that is, the users and groups who are explicitly denied entitlements to run applications published from the desktop group.

This can be used to exclude users or groups or users who would otherwise gain access by groups specified in the included users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Enables or disables the included users filter. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to an application session by the application rule.

Users who would be implicitly granted access when the filter is disabled can still be explicitly denied access using the excluded users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUsers<User[]>

Changes the included users filter of the rule, that is, the users and groups who are granted an entitlement to an application session by the rule.

If a user appears explicitly in the excluded users filter of the rule or is a member of a group that appears in the excluded users filter, no entitlement is granted whether or not the user appears in the included users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveExcludedUsers<User[]>

Removes the specified users from the excluded users filter of the application rule, that is, the users and groups who are explicitly denied entitlements to run applications published from the desktop group.

See the ExcludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveIncludedUsers<User[]>

Removes the specified users from the included users filter of the rule, that is, the users and groups who are granted an entitlement to an application session by the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionReconnection<SessionReconnection>

Defines reconnection (roaming) behavior for sessions launched using this rule. Session reconnection control is an experimental and unsupported feature.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AppEntitlementPolicyRule The application rule in the entitlement policy rule to be modified.

Return Values

None or Citrix.Broker.Admin.SDK.AppEntitlementPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AppEntitlementPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerAppEntitlementPolicyRule 'Temp Workers' -AddIncludedUsers office\contractors
Adds the user group OFFICE\contractors to those entitled to run applications from the rule's associated desktop group. This grants all members of that group an entitlement to an application session from that group.

---------- EXAMPLE 2 ----------

C:\PS> Set-BrokerAppEntitlementPolicyRule 'Temp Workers' -Enabled $false
Disables the Temp Workers application rule in the entitlement policy. This prevents further application sessions being launched using this rule until it is re-enabled. However, access to existing application sessions is not affected.

Set-BrokerApplication

Sep 10, 2014

Changes the settings of an application to the value specified in the command.

Syntax

```
Set-BrokerApplication [-InputObject] <Application[]> [-PassThru] [-BrowserName <String>] [-ClientFolder <String>] [-CommandLineArguments <String>] [-CommandLineExecutable <String>] [-CpuPriorityLevel <CpuPriorityLevel>] [-Description <String>] [-Enabled <Boolean>] [-IconFromClient <Boolean>] [-IconUid <Int32>] [-PublishedName <String>] [-SecureCmdLineArgumentsEnabled <Boolean>] [-ShortcutAddedToDesktop <Boolean>] [-ShortcutAddedToStartMenu <Boolean>] [-StartMenuFolder <String>] [-UserFilterEnabled <Boolean>] [-Visible <Boolean>] [-WaitForPrinterCreation <Boolean>] [-WorkingDirectory <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplication [-Name] <String> [-PassThru] [-BrowserName <String>] [-ClientFolder <String>] [-CommandLineArguments <String>] [-CommandLineExecutable <String>] [-CpuPriorityLevel <CpuPriorityLevel>] [-Description <String>] [-Enabled <Boolean>] [-IconFromClient <Boolean>] [-IconUid <Int32>] [-PublishedName <String>] [-SecureCmdLineArgumentsEnabled <Boolean>] [-ShortcutAddedToDesktop <Boolean>] [-ShortcutAddedToStartMenu <Boolean>] [-StartMenuFolder <String>] [-UserFilterEnabled <Boolean>] [-Visible <Boolean>] [-WaitForPrinterCreation <Boolean>] [-WorkingDirectory <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Set-BrokerApplication cmdlet changes the value of one or more properties of an application, such as its CpuPriorityLevel or its CommandLineArguments, to the value specified in the command.

This cmdlet lets you change only the settings of the Application object, and not the relationships to other objects. For instance, it does not let you change which users can access this application, or change which desktop groups this application is published to. To do this, you need to remove the existing association, and then add a new association. The following example shows how to change the desktop group that an application is associated with from $group1 to $group2:

```
Remove-BrokerApplication -DesktopGroup $group1

Add-RemoveApplication -DesktopGroup $group2
```

You can change properties of both HostedOnDesktop and InstalledOnClient applications but it is not possible to change the ApplicationType. Also, the Name cannot be changed using this cmdlet; to do this, use the Rename-BrokerApplication cmdlet.

Related topics

New-BrokerApplication

Add-BrokerApplication

Get-BrokerApplication

Remove-BrokerApplication

Rename-BrokerApplication

Move-BrokerApplication

Parameters

-InputObject<Application[]>

Specifies the application to modify. The Uid of the application can also be substituted for the object.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the application to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-BrowserName<String>

Specifies the name of the application to modify. Note that the BrowserName cannot be changed in this manner; to modify the BrowserName of an application, use the Rename-BrokerApplication cmdlet.

Required?	false

Default Value	
Accept Pipeline Input?	false

-ClientFolder<String>

Specifies the folder that the application belongs to as the user sees it. This is the application folder displayed in the Citrix Online Plug-in, in Web Services, and also in the user's start menu. Subdirectories can be specified with '\' character. The following special characters are not allowed: / * ? < > | " :. Note that this property cannot be set for applications of type InstalledOnClient.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CommandLineArguments<String>

Specifies the command-line arguments to use when launching the executable.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CommandLineExecutable<String>

Specifies the name of the executable file to launch.

Required?	false
Default Value	
Accept Pipeline Input?	false

-CpuPriorityLevel<CpuPriorityLevel>

Specifies the CPU priority for the launched executable. Valid values are: Low, BelowNormal, Normal, AboveNormal, and High.

Note that this property cannot be set for applications of type InstalledOnClient.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Specifies the description of the application.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Specifies whether or not this application can be launched.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconFromClient<Boolean>

Specifies if the app icon should be retrieved from the application on the client. This is reserved for possible future use, and all applications of type HostedOnDesktop cannot set or change this value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Specifies which icon to use for this application. This application is visible both to the administrator (in the consoles) and also

to the user. If no icon is specified, then a generic built-in application icon is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Specifies the name seen by end users who have access to this application.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureCmdLineArgumentsEnabled<Boolean>

Specifies whether the command-line arguments should be secured. This is reserved for possible future use, and all applications of type HostedOnDesktop can only have this value set to true.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ShortcutAddedToDesktop<Boolean>

Specifies whether or not a shortcut to the application should be placed on the user device.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ShortcutAddedToStartMenu<Boolean>

Specifies whether a shortcut to the application should be placed in the user's start menu on their user device.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartMenuFolder<String>

Specifies the name of the start menu folder that holds the application shortcut (if any). This is valid only for the Citrix Online Plug-in. Subdirectories can be specified with '\' character. The following special characters are not allowed: / * ? < > | " :.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserFilterEnabled<Boolean>

Specifies whether the application's user filter is enabled or disabled. Where the user filter is enabled, the application is only visible to users who appear in the filter (either explicitly or by virtue of group membership).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Visible<Boolean>

Specifies whether or not this application is visible to users. Note that it's possible for an application to be disabled and still visible.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WaitForPrinterCreation<Boolean>

Specifies whether or not the session waits for the printers to be created before allowing the end-user to interact with the session. Note that this property cannot be set for applications of type InstalledOnClient.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WorkingDirectory<String>

Specifies from which working directory the executable is launched from.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.

Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Application, or depends on parameter You can pipe the application to be added to Set-BrokerApplication. You can also pipe some of the other parameters by name.

Return Values

None or Citrix.Broker.Admin.SDK.Application

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.Application object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerApplication -Name "Notepad" -Description 'Windows Notepad'
```

Modifies the application that has a Name of "Notepad" so that its description reads Windows Notepad.

---------- EXAMPLE 2 ----------

```
C:\PS> $app = Get-BrokerApplication -BrowserName "Calculator"
C:\PS> Set-BrokerApplication -InputObject $app -Enabled $false
```

First gets the application with a BrowserName of "Calculator", then modifies that application (by supplying the application object in the first position) so that it is disabled for users.

Set-BrokerApplicationInstanceMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for ApplicationInstance

Syntax

Set-BrokerApplicationInstanceMetadata [-ApplicationInstanceId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationInstanceMetadata [-ApplicationInstanceId] <Int64> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationInstanceMetadata [-ApplicationInstanceId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationInstanceMetadata [-InputObject] <ApplicationInstance[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationInstanceMetadata [-InputObject] <ApplicationInstance[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerApplicationInstanceMetadata cmdlet creates/updates metadata key-value pairs for ApplicationInstance. The ApplicationInstance can be specified by InputObject or piping.

Related topics

Parameters

-ApplicationInstanceId<Int64>

Specifies the ApplicationInstance object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-InputObject<ApplicationInstance[]>

Specifies the ApplicationInstance objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerApplicationInstance You can pipe the ApplicationInstance to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerApplicationInstance

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerApplicationInstance object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerApplicationInstanceMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the ApplicationInstance whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerApplicationInstance | Set-BrokerApplicationInstanceMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the ApplicationInstance in the site

Set-BrokerApplicationMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for Application

Syntax

Set-BrokerApplicationMetadata [-ApplicationId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationMetadata [-ApplicationId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationMetadata [-ApplicationId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationMetadata [-InputObject] <Application[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationMetadata [-InputObject] <Application[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationMetadata [-ApplicationName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerApplicationMetadata [-ApplicationName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerApplicationMetadata cmdlet creates/updates metadata key-value pairs for Application. The Application can be specified by InputObject or piping.

Related topics

Parameters

-ApplicationId<Int32>

Specifies the Application object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-InputObject<Application[]>

Specifies the Application objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-ApplicationName<String>

Specifies the Application object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerApplication You can pipe the Application to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerApplication

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerApplication object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerApplicationMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the Application whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerApplication | Set-BrokerApplicationMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the Application in the site

---------- EXAMPLE 3 ----------

C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerApplicationMetadata 'objname'
This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the Application in the site whose name is 'objname'

Set-BrokerAssignmentPolicyRule

Sep 10, 2014

Modifies an existing desktop rule in the site's assignment policy.

Syntax

```
Set-BrokerAssignmentPolicyRule [-InputObject] <AssignmentPolicyRule[]> [-PassThru] [-AddExcludedUsers <User[]>] [-AddIncludedUsers <User[]>] [-ColorDepth <ColorDepth>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IconUid <Int32>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-MaxDesktops <Int32>] [-PublishedName <String>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedUsers <User[]>] [-SecureIcaRequired <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAssignmentPolicyRule [-Name] <String> [-PassThru] [-AddExcludedUsers <User[]>] [-AddIncludedUsers <User[]>] [-ColorDepth <ColorDepth>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IconUid <Int32>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-MaxDesktops <Int32>] [-PublishedName <String>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedUsers <User[]>] [-SecureIcaRequired <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Set-BrokerAssignmentPolicyRule cmdlet modifies an existing desktop rule in the site's assignment policy.

A desktop rule in the assignment policy defines the users who are entitled to self-service persistent machine assignments from the rule's desktop group. A rule defines how many machines a user is allowed from the group for delivery of full desktop sessions.

Changing a desktop rule does not alter machine assignments that have already been made by the rule, nor does it affect active sessions to those machines in any way.

Related topics

New-BrokerAssignmentPolicyRule

Get-BrokerAssignmentPolicyRule

Rename-BrokerAssignmentPolicyRule

Remove-BrokerAssignmentPolicyRule

Parameters

-InputObject<AssignmentPolicyRule[]>

The desktop rule in the assignment policy to be modified.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the desktop rule in the assignment policy to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-AddExcludedUsers<User[]>

Adds the specified users to the excluded users filter of the rule, that is, the users and groups who are explicitly denied an entitlement to a machine assignment from this rule.

See the ExcludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddIncludedUsers<User[]>

Adds the specified users to the included users filter of the rule, that is, the users and groups who are granted an entitlement to a machine assignment by the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Changes the color depth of any desktop sessions to machines assigned by the rule.

Valid values are $null, FourBit, EightBit, SixteenBit, and TwentyFourBit.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Changes the description of the desktop rule. The text may be visible to the end user, for example, as a tooltip associated with the desktop entitlement.

A null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Enables or disables the desktop rule. A disabled rule is ignored when evaluating the site's assignment policy.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Enables or disables the excluded users filter. If the filter is disabled then any user entries in the filter are ignored when assignment policy rules are evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUsers<User[]>

Changes the excluded users filter of the desktop rule, that is, the users and groups who are explicitly denied an entitlement to a machine assignment from this rule.

This can be used to exclude users or groups who would otherwise gain access by groups specified in the included users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Changes the unique ID of the icon used to display the machine assignment entitlement to the user, and of the assigned desktop itself following the assignment.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Enables or disables the included users filter. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to a machine assignment by the rule.

Users who would be implicitly granted access when the filter is disabled can still be explicitly denied access using the excluded users filter.

For rules that relate to RemotePC desktop groups however, if the included user filter is disabled, the rule is effectively disabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUsers<User[]>

Changes the included users filter of the rule, that is, the users and groups who are granted an entitlement to a machine assignment by the rule.

If a user appears explicitly in the excluded users filter of the rule, or is a member of a group that appears in the excluded users filter, no entitlement is granted whether or not the user appears in the included users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxDesktops<Int32>

The number of machines from the rule's desktop group to which a user is entitled. Where an entitlement is granted to a user group rather than an individual, the number of machines applies to each member of the user group independently.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Changes the published name of the machine assignment entitlement as seen by the user. Changing the published name does not affect the names of desktops that have already been assigned by the rule.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveExcludedUsers<User[]>

Removes the specified users from the excluded users filter of the rule, that is, the users and groups who are explicitly denied an entitlement to a machine assignment from this rule.

See the ExcludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveIncludedUsers<User[]>

Removes the specified users from the included users filter of the desktop rule, that is, the users and groups who are granted an entitlement to a machine assignment by the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Changes whether the desktop rule requires the SecureICA protocol for desktop sessions to machines assigned using the entitlement.

The default null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	

Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.AssignmentPolicyRule The desktop rule within the assignment policy to be modified.

Return Values

None or Citrix.Broker.Admin.SDK.AssignmentPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.AssignmentPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerAssignmentPolicyRule 'Temp Staff' -AddIncludedUsers office\interns
Adds the user group OFFICE\interns to the Temp Staff desktop rule in the assignment policy. This grants all members of that user group entitlements to machines in the rule's desktop group. The number of machine entitlements per user and the session properties of the desktops obtained using the rule are determined by the rule's other properties.

---------- EXAMPLE 2 ----------

```
C:\PS> Set-BrokerAssignmentPolicyRule 'Temp Staff' -Enabled $false
```

Disables the Temp Staff desktop rule in the assignment policy. This prevents further machine assignments being made using this rule until it is re-enabled. However, access to machines already assigned using the rule is not impacted.

Set-BrokerAssignmentPolicyRuleMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for AssignmentPolicyRule

Syntax

Set-BrokerAssignmentPolicyRuleMetadata [-AssignmentPolicyRuleId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAssignmentPolicyRuleMetadata [-AssignmentPolicyRuleId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAssignmentPolicyRuleMetadata [-AssignmentPolicyRuleId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAssignmentPolicyRuleMetadata [-InputObject] <AssignmentPolicyRule[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAssignmentPolicyRuleMetadata [-InputObject] <AssignmentPolicyRule[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAssignmentPolicyRuleMetadata [-AssignmentPolicyRuleName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerAssignmentPolicyRuleMetadata [-AssignmentPolicyRuleName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerAssignmentPolicyRuleMetadata cmdlet creates/updates metadata key-value pairs for AssignmentPolicyRule. The AssignmentPolicyRule can be specified by InputObject or piping.

Related topics

Parameters

-AssignmentPolicyRuleId<Int32>

Specifies the AssignmentPolicyRule object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-InputObject<AssignmentPolicyRule[]>

Specifies the AssignmentPolicyRule objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AssignmentPolicyRuleName<String>

Specifies the AssignmentPolicyRule object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerAssignmentPolicyRule You can pipe the AssignmentPolicyRule to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerAssignmentPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerAssignmentPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerAssignmentPolicyRuleMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the AssignmentPolicyRule whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerAssignmentPolicyRule | Set-BrokerAssignmentPolicyRuleMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the AssignmentPolicyRule in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerAssignmentPolicyRuleMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the AssignmentPolicyRule in the site whose name is 'objname'

Set-BrokerCatalog

Sep 10, 2014

Sets the properties of a catalog.

Syntax

Set-BrokerCatalog [-InputObject] <Catalog[]> [-PassThru] [-Description <String>] [-IsRemotePC <Boolean>] [-MinimumFunctionalLevel <FunctionalLevel>] [-ProvisioningSchemeId <Guid>] [-PvsAddress <String>] [-PvsDomain <String>] [-RemotePCHypervisorConnectionUid <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerCatalog [-Name] <String> [-PassThru] [-Description <String>] [-IsRemotePC <Boolean>] [-MinimumFunctionalLevel <FunctionalLevel>] [-ProvisioningSchemeId <Guid>] [-PvsAddress <String>] [-PvsDomain <String>] [-RemotePCHypervisorConnectionUid <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerCatalog cmdlet sets properties of a catalog or set of catalogs. The catalog can be specified by name, in which case only one catalog can be specified, or one or more catalog instances can be passed to the command either by piping or by using the -InputObject parameter.

Related topics

Get-BrokerCatalog

New-BrokerCatalog

Remove-BrokerCatalog

Rename-BrokerCatalog

Parameters

-InputObject<Catalog[]>

Specifies the catalog objects to modify.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Identifies the catalog to modify.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-Description<String>

Supplies the new value of the Description property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsRemotePC<Boolean>

Supplies a new value for IsRemotePC.

IsRemotePC can only be enabled when:

o SessionSupport is SingleSession

o MachinesArePhysical is true.

IsRemotePC can only be set from true to false when no RemotePCAccount references this catalog, and when no Remote PC relationship exists between this catalog and a desktop group.

Required?	false
Default Value	

Accept Pipeline Input?	false

-MinimumFunctionalLevel<FunctionalLevel>

The new minimum FunctionalLevel required for machines to work successfully in the catalog. If this is higher than the FunctionalLevel of any machines already in the catalog, they will immediately cease to function.

Valid values are L5, L7, L7_6

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningSchemeId<Guid>

Specifies the identity of the MCS provisioning scheme the catalog is associated with (can only be specified for new catalogs with a ProvisioningType of MCS; once set can never be changed).

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvsAddress<String>

Supplies the new value of the PvsAddress property. Can only be set if CatalogKind is Pvs or PvsPvd.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PvsDomain<String>

Supplies the new value of the PvsDomain property. Can only be set if CatalogKind is PvsPvd.

Required?	false

Default Value	
Accept Pipeline Input?	false

-RemotePCHypervisorConnectionUid<Int32>

Supplies the new hypervisor connection to use for powering on remote PCs in this catalog (only allowed when IsRemotePC is true); this will affect all machines already in the catalog as well as those created later.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Catalog You can pipe the catalogs to be modified to Set-BrokerCatalog.

Return Values

None or Citrix.Broker.Admin.SDK.Catalog

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.Catalog object.

Notes

A catalog's Name property cannot be changed by Set-BrokerCatalog. To rename a catalog use Rename-BrokerCatalog.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -Description "New Description"
```

This example specifies a catalog by name and sets its description.

-------------------------- EXAMPLE 2 --------------------------

```
C:\PS> $permCatalogs = Get-BrokerCatalog -AllocationType Static
C:\PS> Set-BrokerCatalog -InputObject $permCatalogs -Description "Permanently assigned machines"
```

This example sets the description for all catalogs with AllocationType 'Static'.

Set-BrokerCatalogMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for Catalog

Syntax

Set-BrokerCatalogMetadata [-CatalogId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerCatalogMetadata [-CatalogId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerCatalogMetadata [-CatalogId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerCatalogMetadata [-InputObject] <Catalog[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerCatalogMetadata [-InputObject] <Catalog[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerCatalogMetadata [-CatalogName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerCatalogMetadata [-CatalogName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerCatalogMetadata cmdlet creates/updates metadata key-value pairs for Catalog. The Catalog can be specified by InputObject or piping.

Related topics

Parameters

-CatalogId<Int32>

Specifies the Catalog object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Catalog[]>

Specifies the Catalog objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-CatalogName<String>

Specifies the Catalog object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerCatalog You can pipe the Catalog to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerCatalog

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerCatalog object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerCatalogMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the Catalog whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerCatalog | Set-BrokerCatalogMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the Catalog in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerCatalogMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the Catalog in the site whose name is 'objname'

Set-BrokerConfigurationSlotMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for ConfigurationSlot

Syntax

Set-BrokerConfigurationSlotMetadata [-ConfigurationSlotId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerConfigurationSlotMetadata [-ConfigurationSlotId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerConfigurationSlotMetadata [-ConfigurationSlotId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerConfigurationSlotMetadata [-InputObject] <ConfigurationSlot[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerConfigurationSlotMetadata [-InputObject] <ConfigurationSlot[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerConfigurationSlotMetadata [-ConfigurationSlotName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerConfigurationSlotMetadata [-ConfigurationSlotName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerConfigurationSlotMetadata cmdlet creates/updates metadata key-value pairs for ConfigurationSlot. The ConfigurationSlot can be specified by InputObject or piping.

Related topics

Parameters

-ConfigurationSlotId<Int32>

Specifies the ConfigurationSlot object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-InputObject<ConfigurationSlot[]>

Specifies the ConfigurationSlot objects whose Metadata is to be created/updated.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-ConfigurationSlotName<String>

Specifies the ConfigurationSlot object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerConfigurationSlot You can pipe the ConfigurationSlot to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerConfigurationSlot

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerConfigurationSlot object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerConfigurationSlotMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the ConfigurationSlot whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerConfigurationSlot | Set-BrokerConfigurationSlotMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the ConfigurationSlot in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerConfigurationSlotMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the ConfigurationSlot in the site whose name is 'objname'

Set-BrokerControllerMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for Controller

Syntax

Set-BrokerControllerMetadata [-ControllerId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerControllerMetadata [-ControllerId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerControllerMetadata [-ControllerId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerControllerMetadata [-InputObject] <Controller[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerControllerMetadata [-InputObject] <Controller[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerControllerMetadata [-ControllerName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerControllerMetadata [-ControllerName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerControllerMetadata cmdlet creates/updates metadata key-value pairs for Controller. The Controller can be specified by InputObject or piping.

Related topics

Parameters

-ControllerId<Int32>

Specifies the Controller object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-InputObject<Controller[]>

Specifies the Controller objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-ControllerName<String>

Specifies the Controller object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerController You can pipe the Controller to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerController

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerController object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerControllerMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the Controller whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerController | Set-BrokerControllerMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the Controller in the site

---------- EXAMPLE 3 ----------

C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerControllerMetadata 'objname'
This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the Controller in the site whose name is 'objname'

Set-BrokerDBConnection

Sep 10, 2014

Configures a database connection for the Broker Service.

Syntax

```
Set-BrokerDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [[-Force]] [<CommonParameters>]
```

Detailed Description

Specifies the database connection string for use by the currently selected Citrix Broker Service instance.

The service records the connection string and attempts to contact the specified database. If the database cannot initially be contacted the service retries the connection at intervals until contact with the database is successfully established.

Is is not possible to set a new database connection string for the service if one is already recorded. The connection string must first be set to $null. This action causes the service to reset and return to its idle state, at which point a new connection string can be set.

When a database connection string is successfully set for the service, a status of OK is returned by the cmdlet. If the database connection string is set to $null, a DBUnconfigured status is returned.

A syntactically invalid connection string is not recorded.

Only use of Windows authentication within the connection string is supported; a connection string containing SQL authentication credentials is always rejected as invalid.

The current service instance is the one on the local machine, or the one most recently specified using the -AdminAddress parameter of a Broker SDK cmdlet.

Related topics

Get-BrokerServiceStatus

Get-BrokerDBConnection

Test-BrokerDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the Broker Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-BrokerDBConnection cmdlet returns an object describing the status of the Broker Service together with extra diagnostics information. Possible values are:

-- OK:

The Broker Service instance is configured with a valid database and service schema. The service is operational.

-- DBUnconfigured:

No database connection string is set for the Broker Service instance.

-- DBRejectedConnection:

The database rejected the logon attempt from the Broker Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

-- InvalidDBConfigured:

The specified database does not exist, is not visible to the Broker Service instance, or the service's schema within the database is invalid.

-- DBNotFound:

The specified database could not be located with the configured connection string.

-- DBNewerVersionThanService:

The version of the Broker Service currently in use is newer than, and incompatible with, the version of the Broker Service schema on the database. Upgrade the Broker Service to a more recent version.

-- DBOlderVersionThanService:

The version of the Broker Service schema on the database is newer than, and incompatible with, the version of the Broker Service currently in use. Upgrade the database schema to a more recent version.

-- DBVersionChangeInProgress:

A database schema upgrade is in progress.

-- PendingFailure:

Connectivity between the Broker Service instance and the database has been lost. This may be a transitory network error, but may indicate a loss of connectivity that requires administrator intervention.

-- Failed:

Connectivity between the Broker Service instance and the database has been lost for an extended period of time, or has failed due to a configuration problem. The service instance cannot operate while its connection to the database is unavailable.

-- Unknown:

The status of the Broker Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

C:\PS>Set-BrokerDBConnection "Server=dbserver\SQLEXPRESS;Database=XDDB;Trusted_Connection=True"
Configures the service instance to use a database called XDDB on an SQL Server Express database running on the machine called dbserver. Integrated Windows authentication is required.

-------------------------- EXAMPLE 2 --------------------------

C:\PS>Set-BrokerDBConnection -DBConnection $null
Resets the service instance's database connection string. The service instance resets and returns to an idle state until a valid new database connection string is specified.

Set-BrokerDesktopGroup

Sep 10, 2014

Adjusts the settings of a broker desktop group.

Syntax

Set-BrokerDesktopGroup [-InputObject] <DesktopGroup[]> [-PassThru] [-AutomaticPowerOnForAssigned <Boolean>] [-AutomaticPowerOnForAssignedDuringPeak <Boolean>] [-ColorDepth <ColorDepth>] [-DeliveryType <DeliveryType>] [-Description <String>] [-Enabled <Boolean>] [-IconUid <Int32>] [-InMaintenanceMode <Boolean>] [-IsRemotePC <Boolean>] [-MinimumFunctionalLevel <FunctionalLevel>] [-OffPeakBufferSizePercent <Int32>] [-OffPeakDisconnectAction <SessionChangeHostingAction>] [-OffPeakDisconnectTimeout <Int32>] [-OffPeakExtendedDisconnectAction <SessionChangeHostingAction>] [-OffPeakExtendedDisconnectTimeout <Int32>] [-OffPeakLogOffAction <SessionChangeHostingAction>] [-OffPeakLogOffTimeout <Int32>] [-PeakBufferSizePercent <Int32>] [-PeakDisconnectAction <SessionChangeHostingAction>] [-PeakDisconnectTimeout <Int32>] [-PeakExtendedDisconnectAction <SessionChangeHostingAction>] [-PeakExtendedDisconnectTimeout <Int32>] [-PeakLogOffAction <SessionChangeHostingAction>] [-PeakLogOffTimeout <Int32>] [-ProtocolPriority <String[]>] [-PublishedName <String>] [-SecureIcaRequired <Boolean>] [-SettlementPeriodBeforeAutoShutdown <TimeSpan>] [-ShutdownDesktopsAfterUse <Boolean>] [-TimeZone <String>] [-TurnOnAddedMachine <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerDesktopGroup [-Name] <String> [-PassThru] [-AutomaticPowerOnForAssigned <Boolean>] [-AutomaticPowerOnForAssignedDuringPeak <Boolean>] [-ColorDepth <ColorDepth>] [-DeliveryType <DeliveryType>] [-Description <String>] [-Enabled <Boolean>] [-IconUid <Int32>] [-InMaintenanceMode <Boolean>] [-IsRemotePC <Boolean>] [-MinimumFunctionalLevel <FunctionalLevel>] [-OffPeakBufferSizePercent <Int32>] [-OffPeakDisconnectAction <SessionChangeHostingAction>] [-OffPeakDisconnectTimeout <Int32>] [-OffPeakExtendedDisconnectAction <SessionChangeHostingAction>] [-OffPeakExtendedDisconnectTimeout <Int32>] [-OffPeakLogOffAction <SessionChangeHostingAction>] [-OffPeakLogOffTimeout <Int32>] [-PeakBufferSizePercent <Int32>] [-PeakDisconnectAction <SessionChangeHostingAction>] [-PeakDisconnectTimeout <Int32>] [-PeakExtendedDisconnectAction <SessionChangeHostingAction>] [-PeakExtendedDisconnectTimeout <Int32>] [-PeakLogOffAction <SessionChangeHostingAction>] [-PeakLogOffTimeout <Int32>] [-ProtocolPriority <String[]>] [-PublishedName <String>] [-SecureIcaRequired <Boolean>] [-SettlementPeriodBeforeAutoShutdown <TimeSpan>] [-ShutdownDesktopsAfterUse <Boolean>] [-TimeZone <String>] [-TurnOnAddedMachine <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerDesktopGroup cmdlet is used to disable or enable an existing broker desktop group or to alter its settings.

Related topics

Get-BrokerDesktopGroup

New-BrokerDesktopGroup

Rename-BrokerDesktopGroup

Remove-BrokerDesktopGroup

Parameters

-InputObject<DesktopGroup[]>

Specifies the desktop groups to adjust.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the desktop groups to adjust, based on their Name property.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-AutomaticPowerOnForAssigned<Boolean>

Specifies whether assigned desktops in the desktop group should be automatically started at the start of peak time periods. Only relevant for groups whose DesktopKind is Private.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AutomaticPowerOnForAssignedDuringPeak<Boolean>

Specifies whether assigned desktops in the desktop group should be automatically started throughout peak time periods. Only relevant for groups whose DesktopKind is Private and which have AutomaticPowerOnForAssigned set to true.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Specifies the color depth that the ICA session should use for desktops in this group. Valid values are FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DeliveryType<DeliveryType>

Specifies whether desktops, applications, or both, can be delivered from machines contained within the desktop group. Desktop groups with a DesktopKind of Private cannot be used to deliver both desktops and applications.

When changing the delivery type to desktops only, there must be no remaining desktop-hosted applications associated with the group, or application-specific assignment/entitlement policy rules for the group.

When changing the delivery type to applications only, there must be no remaining client-hosted applications associated with the group, or desktop-specific assignment/entitlement policy rules for the group.

Valid values are DesktopsOnly, AppsOnly, and DesktopsAndApps.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

A description for this desktop group useful for administrators of the site.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Whether the desktop group should be in the enabled state; disabled desktop groups do not appear to users.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

The UID of the broker icon to be displayed to users for their desktop(s) in this desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Whether the desktop should be put into maintenance mode; a desktop group in maintenance mode will not allow users to connect or reconnect to their desktops.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsRemotePC<Boolean>

Supplies a new value for IsRemotePC.

IsRemotePC can only be enabled when:

o SessionSupport is SingleSession

o DeliveryType is DesktopsOnly

o DesktopKind is Private

IsRemotePC can be switched from true to false only if no RemotePC relationship exists between a catalog and this desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MinimumFunctionalLevel<FunctionalLevel>

The new minimum FunctionalLevel required for machines to work successfully in the desktop group. If this is higher than the FunctionalLevel of any machines already in the desktop group, they will immediately cease to function.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakBufferSizePercent<Int32>

The percentage of machines in the desktop group that should be kept available in an idle state outside peak hours.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakDisconnectAction<SessionChangeHostingAction>

The action to be performed after a configurable period of a user session disconnecting outside peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakDisconnectTimeout<Int32>

The number of minutes before the configured action should be performed after a user session disconnects outside peak hours.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakExtendedDisconnectAction<SessionChangeHostingAction>

The action to be performed after a second configurable period of a user session disconnecting outside peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakExtendedDisconnectTimeout<Int32>

The number of minutes before the second configured action should be performed after a user session disconnects outside peak hours.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakLogOffAction<SessionChangeHostingAction>

The action to be performed after a configurable period of a user session ending outside peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OffPeakLogOffTimeout<Int32>

The number of minutes before the configured action should be performed after a user session ends outside peak hours.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakBufferSizePercent<Int32>

The percentage of machines in the desktop group that should be kept available in an idle state in peak hours.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakDisconnectAction<SessionChangeHostingAction>

The action to be performed after a configurable period of a user session disconnecting in peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakDisconnectTimeout<Int32>

The number of minutes before the configured action should be performed after a user session disconnects in peak hours.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakExtendedDisconnectAction<SessionChangeHostingAction>

The action to be performed after a second configurable period of a user session disconnecting in peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakExtendedDisconnectTimeout<Int32>

The number of minutes before the second configured action should be performed after a user session disconnects in peak hours.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakLogOffAction<SessionChangeHostingAction>

The action to be performed after a configurable period of a user session ending in peak hours. Possible values are Nothing, Suspend, or Shutdown.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakLogOffTimeout<Int32>

The number of minutes before the configured action should be performed after a user session ends in peak hours.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProtocolPriority<String[]>

A list of protocol names in the order in which they should be attempted for use during connection.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

The name that will be displayed to users for their desktop(s) in this desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Whether HDX connections to desktops in the new desktop group require the use of a secure protocol.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SettlementPeriodBeforeAutoShutdown<TimeSpan>

Time after a session ends during which automatic shutdown requests (for example, shutdown after use, idle pool management) are deferred. Any outstanding shutdown request takes effect after the settlement period expires. This is typically used to configure time to allow logoff scripts to complete.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ShutdownDesktopsAfterUse<Boolean>

Whether desktops in this desktop group should be automatically shut down when each user session completes (only relevant to power-managed desktops).

Required?	false
Default Value	
Accept Pipeline Input?	false

-TimeZone<String>

The time zone in which this desktop group's machines reside.

The time zone must be specified for any of the group's automatic power management settings to take effect. Automatic power management operations include pool management (power time schemes), reboot schedules, session disconnect and logoff actions, and powering on assigned machines etc.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TurnOnAddedMachine<Boolean>

This flag specifies whether the Broker Service should attempt to power on machines when they are added to the desktop group.

Required?	false

Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.DesktopGroup You can pipe the desktop groups to be adjusted to Set-BrokerDesktopGroup.

Return Values

None or Citrix.Broker.Admin.SDK.DesktopGroup

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.DesktopGroup object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerDesktopGroup EMEA* -InMaintenanceMode $true -PassThru
```

Sets all desktop groups with names starting "EMEA" into maintenance mode, returning the set of desktop groups.

-------------------------- EXAMPLE 2 --------------------------

```
C:\PS> Get-BrokerDesktopGroup -InMaintenanceMode $true | Set-BrokerDesktopGroup -Enabled $false
```

Disable all desktop groups that are in maintenance mode.

Set-BrokerDesktopGroupMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for DesktopGroup

Syntax

Set-BrokerDesktopGroupMetadata [-DesktopGroupId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerDesktopGroupMetadata [-DesktopGroupId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerDesktopGroupMetadata [-DesktopGroupId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerDesktopGroupMetadata [-InputObject] <DesktopGroup[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerDesktopGroupMetadata [-InputObject] <DesktopGroup[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerDesktopGroupMetadata [-DesktopGroupName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerDesktopGroupMetadata [-DesktopGroupName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerDesktopGroupMetadata cmdlet creates/updates metadata key-value pairs for DesktopGroup. The DesktopGroup can be specified by InputObject or piping.

Related topics

Parameters

-DesktopGroupId<Int32>

Specifies the DesktopGroup object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<DesktopGroup[]>

Specifies the DesktopGroup objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroupName<String>

Specifies the DesktopGroup object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerDesktopGroup You can pipe the DesktopGroup to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerDesktopGroup

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerDesktopGroup object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerDesktopGroupMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the DesktopGroup whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerDesktopGroup | Set-BrokerDesktopGroupMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the DesktopGroup in the site

---------- EXAMPLE 3 ----------

C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerDesktopGroupMetadata 'objname'
This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the DesktopGroup in the site whose name is 'objname'

Set-BrokerEntitlementPolicyRule

Sep 10, 2014

Modifies an existing desktop rule in the site's entitlement policy.

Syntax

Set-BrokerEntitlementPolicyRule [-InputObject] <EntitlementPolicyRule[]> [-PassThru] [-AddExcludedUsers <User[]>] [-AddIncludedUsers <User[]>] [-ColorDepth <ColorDepth>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IconUid <Int32>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-PublishedName <String>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedUsers <User[]>] [-SecureIcaRequired <Boolean>] [-SessionReconnection <SessionReconnection>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerEntitlementPolicyRule [-Name] <String> [-PassThru] [-AddExcludedUsers <User[]>] [-AddIncludedUsers <User[]>] [-ColorDepth <ColorDepth>] [-Description <String>] [-Enabled <Boolean>] [-ExcludedUserFilterEnabled <Boolean>] [-ExcludedUsers <User[]>] [-IconUid <Int32>] [-IncludedUserFilterEnabled <Boolean>] [-IncludedUsers <User[]>] [-PublishedName <String>] [-RemoveExcludedUsers <User[]>] [-RemoveIncludedUsers <User[]>] [-SecureIcaRequired <Boolean>] [-SessionReconnection <SessionReconnection>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerEntitlementPolicyRule cmdlet modifies an existing desktop rule in the site's entitlement policy.

A desktop rule in the entitlement policy defines the users who are allowed per-session access to a machine from the rule's associated desktop group to run a full desktop session.

Changing a rule does not affect existing sessions launched using the rule, but if the change removes an entitlement to a machine that was previously granted, users may be unable to reconnect to a disconnected session on that machine.

Related topics

New-BrokerEntitlementPolicyRule

Get-BrokerEntitlementPolicyRule

Rename-BrokerEntitlementPolicyRule

Remove-BrokerEntitlementPolicyRule

Parameters

-InputObject<EntitlementPolicyRule[]>

The desktop rule in the entitlement policy to be modified.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The name of the desktop rule in the entitlement policy to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-AddExcludedUsers<User[]>

Adds the specified users to the excluded users filter of the rule, that is, the users and groups who are explicitly denied an entitlement to a desktop session from this rule.

See the ExcludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AddIncludedUsers<User[]>

Adds the specified users to the included users filter of the rule, that is, the users and groups who are granted an entitlement to a desktop session by the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Changes the color depth of any desktop sessions launched by a user from this entitlement. Existing sessions are not affected.

Valid values are $null, FourBit, EightBit, SixteenBit, and TwentyFourBit.

A null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Changes the description of the desktop rule. The text may be visible to the end user, for example, as a tooltip associated with the desktop entitlement.

A null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Enables or disables the desktop rule. A disabled rule is ignored when evaluating the site's entitlement policy.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ExcludedUserFilterEnabled<Boolean>

Enables or disables the excluded users filter. If the filter is disabled then any user entries in the filter are ignored when entitlement policy rules are evaluated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ExcludedUsers<User[]>

Changes the excluded users filter of the desktop rule, that is, the users and groups who are explicitly denied an entitlement to a desktop session from this rule.

This can be used to exclude users or groups who would otherwise gain access by groups specified in the included users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Changes the icon (identified by its unique ID) for the published desktop entitlement as seen by the user.

A null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUserFilterEnabled<Boolean>

Enables or disables the included users filter. If the filter is disabled then any user who satisfies the requirements of the access policy is implicitly granted an entitlement to a desktop session by the rule.

Users who would be implicitly granted access when the filter is disabled can still be explicitly denied access using the excluded users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IncludedUsers<User[]>

Changes the included users filter of the desktop rule, that is, the users and groups who are granted an entitlement to a desktop session by the rule.

If a user appears explicitly in the excluded users filter of the rule or is a member of a group that appears in the excluded users filter, no entitlement is granted whether or not the user appears in the included users filter.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Changes the name of the published desktop entitlement as seen by the user.

A null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RemoveExcludedUsers<User[]>

Removes the specified users from the excluded users filter of the rule, that is, the users and groups who are explicitly denied an entitlement to a desktop session from this rule.

See the ExcludedUsers parameter for more information.

Required?	false

Default Value	
Accept Pipeline Input?	false

-RemoveIncludedUsers<User[]>

Removes the specified users from the included users filter of the desktop rule, that is, the users and groups who are granted an entitlement to a desktop session by the rule.

See the IncludedUsers parameter for more information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Changes whether the desktop rule requires the SecureICA protocol for desktop sessions launched using the entitlement.

A null value indicates that the equivalent setting from the rule's desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SessionReconnection<SessionReconnection>

Defines reconnection (roaming) behavior for sessions launched using this rule. Session reconnection control is an experimental and unsupported feature.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.EntitlementPolicyRule The desktop rule in the entitlement policy to be modified.

Return Values

None or Citrix.Broker.Admin.SDK.EntitlementPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.EntitlementPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerEntitlementPolicyRule 'Temp Workers' -AddIncludedUsers office\contractors
Adds the user group OFFICE\contractors to the Temp Workers desktop rule of the entitlement policy. This grants all members of that group an entitlement to a desktop session in the rule's associated desktop group. The session properties of the desktops obtained using the rule are determined by the rule's other properties.

---------- EXAMPLE 2 ----------

C:\PS> Set-BrokerEntitlementPolicyRule 'Temp Workers' -Enabled $false
Disables the Temp Workers desktop rule in the entitlement policy. This prevents further desktop sessions being launched using this rule until it is re-enabled. However, access to existing desktop sessions is not affected.

Set-BrokerEntitlementPolicyRuleMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for EntitlementPolicyRule

Syntax

Set-BrokerEntitlementPolicyRuleMetadata [-EntitlementPolicyRuleId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerEntitlementPolicyRuleMetadata [-EntitlementPolicyRuleId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerEntitlementPolicyRuleMetadata [-EntitlementPolicyRuleId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerEntitlementPolicyRuleMetadata [-InputObject] <EntitlementPolicyRule[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerEntitlementPolicyRuleMetadata [-InputObject] <EntitlementPolicyRule[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerEntitlementPolicyRuleMetadata [-EntitlementPolicyRuleName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerEntitlementPolicyRuleMetadata [-EntitlementPolicyRuleName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerEntitlementPolicyRuleMetadata cmdlet creates/updates metadata key-value pairs for EntitlementPolicyRule. The EntitlementPolicyRule can be specified by InputObject or piping.

Related topics

Parameters

-EntitlementPolicyRuleId<Int32>

Specifies the EntitlementPolicyRule object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-InputObject<EntitlementPolicyRule[]>

Specifies the EntitlementPolicyRule objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-EntitlementPolicyRuleName<String>

Specifies the EntitlementPolicyRule object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerEntitlementPolicyRule You can pipe the EntitlementPolicyRule to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerEntitlementPolicyRule

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerEntitlementPolicyRule object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerEntitlementPolicyRuleMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the EntitlementPolicyRule whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerEntitlementPolicyRule | Set-BrokerEntitlementPolicyRuleMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the EntitlementPolicyRule in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerEntitlementPolicyRuleMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the EntitlementPolicyRule in the site whose name is 'objname'

Set-BrokerHostingPowerAction

Sep 10, 2014

Changes the priority of one or more pending power actions.

Syntax

Set-BrokerHostingPowerAction [-InputObject] <HostingPowerAction[]> [-PassThru] [-ActualPriority <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHostingPowerAction [-MachineName] <String> [-PassThru] [-ActualPriority <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerHostingPowerAction cmdlet modifies an existing power action in the site's power action queue. The only property of power actions you can change, is the current priority of the action.

For a detailed description of the queuing mechanism, see 'help about_Broker_PowerManagement'.

Related topics

Get-BrokerHostingPowerAction

New-BrokerHostingPowerAction

Remove-BrokerHostingPowerAction

Parameters

-InputObject<HostingPowerAction[]>

The power action whose priority is to be changed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MachineName<String>

Changes the priority of actions that are for machines whose name (of the form domain\machine) matches the specified string.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-ActualPriority<Int32>

Specifies a new priority value for the action in the queue.

This priority is the current action priority; the 'base' or original priority for actions cannot be altered. Numerically lower priority values indicate more important actions that are processed in preference to actions with numerically higher priority settings.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host

name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.HostingPowerAction The power action whose priority is to be changed.

Return Values

None or Citrix.Broker.Admin.SDK.HostingPowerAction

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.HostingPowerAction object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerHostingPowerAction -MachineName 'XD_VDA1' -ActualPriority 25
```

Sets the current priority of actions for the machine called 'XD_VDA1' to 25. Numerically lower priority values indicate more important actions that will be processed in preference to actions with numerically higher priority settings.

Set-BrokerHostingPowerActionMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for HostingPowerAction

Syntax

Set-BrokerHostingPowerActionMetadata [-HostingPowerActionId] <Int64> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHostingPowerActionMetadata [-HostingPowerActionId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHostingPowerActionMetadata [-HostingPowerActionId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHostingPowerActionMetadata [-InputObject] <HostingPowerAction[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHostingPowerActionMetadata [-InputObject] <HostingPowerAction[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHostingPowerActionMetadata [-HostingPowerActionName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHostingPowerActionMetadata [-HostingPowerActionName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerHostingPowerActionMetadata cmdlet creates/updates metadata key-value pairs for HostingPowerAction. The HostingPowerAction can be specified by InputObject or piping.

Related topics

Parameters

-HostingPowerActionId<Int64>

Specifies the HostingPowerAction object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<HostingPowerAction[]>

Specifies the HostingPowerAction objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-HostingPowerActionName<String>

Specifies the HostingPowerAction object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False

Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerHostingPowerAction You can pipe the HostingPowerAction to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerHostingPowerAction

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerHostingPowerAction object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerHostingPowerActionMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the HostingPowerAction whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerHostingPowerAction | Set-BrokerHostingPowerActionMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the HostingPowerAction in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerHostingPowerActionMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the

HostingPowerAction in the site whose name is 'objname'

Set-BrokerHypervisorAlertMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for HypervisorAlert

Syntax

Set-BrokerHypervisorAlertMetadata [-HypervisorAlertId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorAlertMetadata [-HypervisorAlertId] <Int64> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorAlertMetadata [-HypervisorAlertId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorAlertMetadata [-InputObject] <HypervisorAlert[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorAlertMetadata [-InputObject] <HypervisorAlert[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerHypervisorAlertMetadata cmdlet creates/updates metadata key-value pairs for HypervisorAlert. The HypervisorAlert can be specified by InputObject or piping.

Related topics

Parameters

-HypervisorAlertId<Int64>

Specifies the HypervisorAlert object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-InputObject<HypervisorAlert[]>

Specifies the HypervisorAlert objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerHypervisorAlert You can pipe the HypervisorAlert to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerHypervisorAlert

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerHypervisorAlert object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerHypervisorAlertMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the HypervisorAlert whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerHypervisorAlert | Set-BrokerHypervisorAlertMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the HypervisorAlert in the site

Set-BrokerHypervisorConnection

Sep 10, 2014

Sets the properties of a hypervisor connection.

Syntax

Set-BrokerHypervisorConnection [-InputObject] <HypervisorConnection[]> [-PassThru] [-PreferredController <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorConnection [-Name] <String> [-PassThru] [-PreferredController <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerHypervisorConnection cmdlet sets the properties on a hypervisor connection.

Related topics

Get-BrokerHypervisorConnection

New-BrokerHypervisorConnection

Remove-BrokerHypervisorConnection

Parameters

-InputObject<HypervisorConnection[]>

Specifies the hypervisor connection object to adjust.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the hypervisor connection object to adjust.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false

Default Value	False
Accept Pipeline Input?	false

-PreferredController<String>

Supplies the new value of the PreferredController property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.HypervisorConnection You can pipe the hypervisor connection to be modified to Set-BrokerHypervisorConnection.

Return Values

None or Citrix.Broker.Admin.SDK.HypervisorConnection

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.HypervisorConnection object.

Examples

---------- **EXAMPLE 1** ----------

```
c:\PS> $hvConn = Get-BrokerHypervisorConnection -PreferredController "oldController" -Name "Xen Server Connection"
c:\PS> Set-BrokerHypervisorConnection -InputObject $hvConn -PreferredController "newController"
```

Updates the preferred controller for a hypervisor connection.

Set-BrokerHypervisorConnectionMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for HypervisorConnection

Syntax

Set-BrokerHypervisorConnectionMetadata [-HypervisorConnectionId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorConnectionMetadata [-HypervisorConnectionId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorConnectionMetadata [-HypervisorConnectionId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorConnectionMetadata [-InputObject] <HypervisorConnection[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorConnectionMetadata [-InputObject] <HypervisorConnection[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorConnectionMetadata [-HypervisorConnectionName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerHypervisorConnectionMetadata [-HypervisorConnectionName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerHypervisorConnectionMetadata cmdlet creates/updates metadata key-value pairs for HypervisorConnection. The HypervisorConnection can be specified by InputObject or piping.

Related topics

Parameters

-HypervisorConnectionId<Int32>

Specifies the HypervisorConnection object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<HypervisorConnection[]>

Specifies the HypervisorConnection objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-HypervisorConnectionName<String>

Specifies the HypervisorConnection object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerHypervisorConnection You can pipe the HypervisorConnection to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerHypervisorConnection

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerHypervisorConnection object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerHypervisorConnectionMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the HypervisorConnection whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerHypervisorConnection | Set-BrokerHypervisorConnectionMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the HypervisorConnection in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerHypervisorConnectionMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the HypervisorConnection in the site whose name is 'objname'

Set-BrokerIconMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for Icon

Syntax

Set-BrokerIconMetadata [-IconId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerIconMetadata [-IconId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerIconMetadata [-IconId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerIconMetadata [-InputObject] <Icon[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerIconMetadata [-InputObject] <Icon[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerIconMetadata cmdlet creates/updates metadata key-value pairs for Icon. The Icon can be specified by InputObject or piping.

Related topics

Parameters

-IconId<Int32>

Specifies the Icon object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Icon[]>

Specifies the Icon objects whose Metadata is to be created/updated.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False

Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerIcon You can pipe the Icon to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerIcon

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerIcon object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerIconMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the Icon whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerIcon | Set-BrokerIconMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the Icon in the site

Set-BrokerLeaseMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for Lease

Syntax

Set-BrokerLeaseMetadata [-LeaseId] <Int64> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerLeaseMetadata [-LeaseId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerLeaseMetadata [-LeaseId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerLeaseMetadata [-InputObject] <Lease[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerLeaseMetadata [-InputObject] <Lease[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerLeaseMetadata [-LeaseName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerLeaseMetadata [-LeaseName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerLeaseMetadata cmdlet creates/updates metadata key-value pairs for Lease. The Lease can be specified by InputObject or piping.

Related topics

Parameters

-LeaseId<Int64>

Specifies the Lease object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Lease[]>

Specifies the Lease objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LeaseName<String>

Specifies the Lease object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerLease You can pipe the Lease to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerLease

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerLease object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerLeaseMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the Lease whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerLease | Set-BrokerLeaseMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the Lease in the site

---------- EXAMPLE 3 ----------

C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerLeaseMetadata 'objname'
This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the Lease in the site whose name is 'objname'

Set-BrokerMachine

Sep 10, 2014

Sets properties on a machine.

Syntax

Set-BrokerMachine [-InputObject] <Machine[]> [-PassThru] [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-HostedMachineId <String>] [-HypervisorConnectionUid <Int32>] [-InMaintenanceMode <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachine [-MachineName] <String> [-PassThru] [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-HostedMachineId <String>] [-HypervisorConnectionUid <Int32>] [-InMaintenanceMode <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerMachine cmdlet sets properties on a machine or set of machines. You can specify a single machine by name or multiple machine instances can be passed to the command by piping or using the -InputObject parameter.

Related topics

Get-BrokerMachine

New-BrokerMachine

Parameters

-InputObject<Machine[]>

The machine instances whose properties you want to set.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MachineName<String>

The machine whose properties you want to set.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-AssignedClientName<String>

Changes the client name assignment of the machine. Set this to $null to remove the assignment. You can assign machines to multiple users, a single client IP address, or a single client name, but only to one of these categories at a time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedIPAddress<String>

Changes the client IP address assignment of the machine. Set this to $null to remove the assignment. You can assign machines to multiple users, a single client IP address, or a single client name, but only to one of these categories at a time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-HostedMachineId<String>

The unique ID by which the hypervisor recognizes the machine. This may only be set for VMs which are not provisioned by MCS.

Required?	false
Default Value	

Accept Pipeline Input?	false

-HypervisorConnectionUid<Int32>

The hypervisor connection that runs the machine. This may only be set for VMs which are not provisioned by MCS.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Sets whether the machine is in maintenance mode or not. A machine in maintenance mode is not available for new sessions, and for managed machines all automatic power management is disabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Machine You can pipe in the machines whose properties you want to set.

Return Values

None or Citrix.Broker.Admin.SDK.Machine

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.Machine object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerMachine -MachineName 'MyDomain\MyMachine' -HypervisorConnectionUid 3
```

This example specifies a machine by name and sets its hypervisor connection.

---------- EXAMPLE 2 ----------

```
C:\PS> $machines = Get-BrokerMachine -MachineName 'MyDomain\*'
C:\PS> Set-BrokerMachine -InputObject $machines -HypervisorConnectionUid 3
```

This example finds all machines in domain MyDomain and sets their hypervisor connections.

---------- EXAMPLE 3 ----------

```
C:\PS> Get-BrokerMachine -MachineName 'MyDomain\*' | Set-BrokerMachine -HypervisorConnectionUid 3
```

This example also finds all machines in domain MyDomain and sets their hypervisor connections.

Set-BrokerMachineCatalog

Sep 10, 2014

Moves one or more machines into a different catalog.

Syntax

Set-BrokerMachineCatalog [-InputObject] <Machine[]> [-CatalogUid] <Int32> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerMachineCatalog cmdlet is used to move machines into a different catalog. The following properties of the destination catalog must exactly match those of the machine's current catalog otherwise the command fails:

o AllocationType

o ProvisioningType

o PersistUserChanges

o SessionSupport

o IsRemotePC

o MinimumFunctionalLevel

o PhysicalMachines

Changing a machine's catalog does not change the machine's desktop group membership. There is no effect on user sessions present on a machine if its catalog is changed.

Related topics

Set-BrokerMachine

New-BrokerCatalog

Parameters

-InputObject<Machine[]>

The machine instances that are being moved into a different catalog.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-CatalogUid<Int32>

The unique identifier of the catalog into which the machines are being moved.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Machine You can pipe in the machines that are to be moved into a new catalog.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $catalog = Get-BrokerCatalog MarketingMachines
    C:\PS> $machines = Get-BrokerMachine -MachineName 'Marketing\*'
    C:\PS> Set-BrokerMachineCatalog $machines -CatalogUid $cat.Uid
```

This example finds all machines in domain Marketing and moves them into a catalog called MarketingMachines.

Set-BrokerMachineCommandMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for MachineCommand

Syntax

Set-BrokerMachineCommandMetadata [-MachineCommandId] <Int64> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineCommandMetadata [-MachineCommandId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineCommandMetadata [-MachineCommandId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineCommandMetadata [-InputObject] <MachineCommand[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineCommandMetadata [-InputObject] <MachineCommand[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerMachineCommandMetadata cmdlet creates/updates metadata key-value pairs for MachineCommand. The MachineCommand can be specified by InputObject or piping.

Related topics

Parameters

-MachineCommandId<Int64>

Specifies the MachineCommand object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<MachineCommand[]>

Specifies the MachineCommand objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerMachineCommand You can pipe the MachineCommand to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerMachineCommand

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerMachineCommand object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerMachineCommandMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the MachineCommand whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerMachineCommand | Set-BrokerMachineCommandMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the MachineCommand in the site

Set-BrokerMachineConfiguration

Sep 10, 2014

Sets the properties of a machine configuration.

Syntax

Set-BrokerMachineConfiguration [-InputObject] <MachineConfiguration[]> [-PassThru] [-Description <String>] [-Policy <Byte[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineConfiguration [-Name] <String> [-PassThru] [-Description <String>] [-Policy <Byte[]>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Sets the properties of a machine configuration. The encoded settings data must only contain settings that match the SettingsGroup of the associated configuration slot. Use the SDK snap-in that matches the SettingsGroup of the associated configuration slot to generate new encoded settings data or modify existing settings values.

Related topics

New-BrokerMachineConfiguration

Get-BrokerMachineConfiguration

Rename-BrokerMachineConfiguration

Remove-BrokerMachineConfiguration

Add-BrokerMachineConfiguration

Parameters

-InputObject<MachineConfiguration[]>

Machine configuration to modify.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Name of machine configuration to modify.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-Description<String>

New description for the machine configuration.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Policy<Byte[]>

New binary array of encoded settings data.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.

Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.MachineConfiguration Machine configuration to modify.

Return Values

None or Citrix.Broker.Admin.SDK.MachineConfiguration

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.MachineConfiguration object.

Examples

---------- EXAMPLE 1 ----------

```
Set-BrokerMachineConfiguration -Name "UPM\Finance Department" -Policy $newPolicy
```

Use the encoded settings binary data in $newPolicy to update the machine configuration.

---------- EXAMPLE 2 ----------

```
Get-BrokerMachineConfiguration -Name "UPM\*" | Set-BrokerMachineConfiguration -Description "User Profile Management"
```

Assign the description "User Profile Management" to every machine configuration associated with the UPM slot.

Set-BrokerMachineConfigurationMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for MachineConfiguration

Syntax

Set-BrokerMachineConfigurationMetadata [-MachineConfigurationId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineConfigurationMetadata [-MachineConfigurationId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineConfigurationMetadata [-MachineConfigurationId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineConfigurationMetadata [-InputObject] <MachineConfiguration[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineConfigurationMetadata [-InputObject] <MachineConfiguration[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineConfigurationMetadata [-MachineConfigurationName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineConfigurationMetadata [-MachineConfigurationName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerMachineConfigurationMetadata cmdlet creates/updates metadata key-value pairs for MachineConfiguration. The MachineConfiguration can be specified by InputObject or piping.

Related topics

Parameters

-MachineConfigurationId<Int32>

Specifies the MachineConfiguration object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-InputObject<MachineConfiguration[]>

Specifies the MachineConfiguration objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MachineConfigurationName<String>

Specifies the MachineConfiguration object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerMachineConfiguration You can pipe the MachineConfiguration to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerMachineConfiguration

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerMachineConfiguration object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerMachineConfigurationMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
```

This command creates/updates the Metadata "MyMetadataName" key-value pair for the MachineConfiguration whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerMachineConfiguration | Set-BrokerMachineConfigurationMetadata -Name "MyMetadataName" -Value "1234"
```

This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the MachineConfiguration in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerMachineConfigurationMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the MachineConfiguration in the site whose name is 'objname'

Set-BrokerMachineMaintenanceMode

Sep 10, 2014

Sets whether the specified machine(s) are in maintenance mode.

Syntax

```
Set-BrokerMachineMaintenanceMode [-InputObject] <Machine[]> [-MaintenanceMode] <Boolean> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The cmdlet can be used to set whether a machine is in maintenance mode or not. A machine in maintenance mode is not available for new sessions, and for managed machines all automatic power management is disabled.

There are times when it is necessary to disable desktops. You can do this by setting the InMaintenanceMode property of a desktop to $true. This puts it into maintenance mode. The broker excludes single-session desktops in maintenance mode from brokering decisions and does not start new sessions on them. Existing sessions are unaffected. For multi-session desktops in maintenance mode, reconnections to existing sessions are allowed, but no new sessions are created on the machine.

Desktops in maintenance mode are also excluded from automatic power management, although explicit power actions are still performed.

This cmdlet is equivalent to using the Set-BrokerMachine cmdlet to set the value of only the InMaintenanceMode property.

Related topics

Set-BrokerMachine

Parameters

-InputObject<Machine[]>

The machine instances whose InMaintenanceMode property you want to set.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MaintenanceMode<Boolean>

Sets whether the machine is in maintenance mode or not. A machine in maintenance mode is not available for new sessions, and for managed machines all automatic power management is disabled.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Machine You can pipe in the machines whose properties you want to set.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $machines = Get-BrokerMachine -MachineName 'MyDomain\*'
       C:\PS> Set-BrokerMachineMaintenanceMode -InputObject $machines $false
```

This example finds all machines in domain MyDomain and removes them from maintenance mode by setting their InMaintenanceMode property to false.

Set-BrokerMachineMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for Machine

Syntax

Set-BrokerMachineMetadata [-MachineId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineMetadata [-MachineId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineMetadata [-MachineId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineMetadata [-InputObject] <Machine[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineMetadata [-InputObject] <Machine[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineMetadata [-MachineName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerMachineMetadata [-MachineName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerMachineMetadata cmdlet creates/updates metadata key-value pairs for Machine. The Machine can be specified by InputObject or piping.

Related topics

Parameters

-MachineId<Int32>

Specifies the Machine object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-InputObject<Machine[]>

Specifies the Machine objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MachineName<String>

Specifies the Machine object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerMachine You can pipe the Machine to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerMachine

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerMachine object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerMachineMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the Machine whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerMachine | Set-BrokerMachineMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the Machine in the site

---------- EXAMPLE 3 ----------

C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerMachineMetadata 'objname'
This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the Machine in the site whose name is 'objname'

Set-BrokerPowerTimeScheme

Sep 10, 2014

Modifies an existing power time scheme.

Syntax

Set-BrokerPowerTimeScheme [-InputObject] <PowerTimeScheme[]> [-PassThru] [-DaysOfWeek <TimeSchemeDays>] [-DisplayName <String>] [-PeakHours <Boolean[]>] [-PoolSize <Int32[]>] [-PoolUsingPercentage <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerPowerTimeScheme [-Name] <String> [-PassThru] [-DaysOfWeek <TimeSchemeDays>] [-DisplayName <String>] [-PeakHours <Boolean[]>] [-PoolSize <Int32[]>] [-PoolUsingPercentage <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerPowerTimeScheme cmdlet modifies an existing time scheme.

Each power time scheme is associated with a particular desktop group, and covers one or more days of the week, defining which hours of those days are considered peak times and which are off-peak times.In addition, the time scheme defines a pool size value for each hour of the day for the days of the week covered by the time scheme. No one desktop group can be associated with two or more time schemes that cover the same day of the week.

For more information about the power policy mechanism and pool size management, see 'help about_Broker_PowerManagement'.

Related topics

Get-BrokerPowerTimeScheme

Rename-BrokerPowerTimeScheme

New-BrokerPowerTimeScheme

Remove-BrokerPowerTimeScheme

Parameters

-InputObject<PowerTimeScheme[]>

The power time scheme to be changed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Identifies the power time scheme to be changed by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-DaysOfWeek<TimeSchemeDays>

Changes the pattern of days of the week that the time scheme applies to. The pattern of days is specified as a single value or a list of values, where each value refers to either a single day or defined group of days.

Valid values are: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Weekend and Weekdays.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DisplayName<String>

Changes the name that is used by the DesktopStudio console when showing the time scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PeakHours<Boolean[]>

Changes the pattern of hours considered 'peak' vs 'off-peak' for the days covered by the time scheme. A 24-entry array of boolean truth values is expected, where the zeroth entry of the array relates to the time period between midnight and 0:59, the first relates to 1am to 1:59 and so on, with the last array element relating to 11 PM to 11:59. If the flag value is $true it means the associated hour of the day is considered a peak time; if $false it means that it is considered off-peak.

If fewer than 24 values are supplied, the final missing values are assumed to be 'false', and if more than 24 values are supplied, only the first 24 are used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PoolSize<Int32[]>

Changes the requested pool size of running machines at the various hours of the day for the days covered by the time scheme. A 24-entry array of integer values is expected, where the zeroth entry of the array relates to the time period between midnight and 0:59, the first relates to 1am to 1:59 and so on, with the last array element relating to 11 PM to 11:59. The pool size array entry values are either absolute numbers of machines that should be running or are a percentage of the machines in the desktop group that should be running during the associated hour of the day. A value of -1 in the array signifies that no management of the number of running machines should be attempted during the associated hour of the day.

If fewer than 24 values are supplied, the final missing values are assumed to be -1, and if more than 24 values are supplied, only the first 24 are used.

Required?	false

Default Value	
Accept Pipeline Input?	false

-PoolUsingPercentage<Boolean>

Changes whether pool size values from the 'PoolSize' array are evaluated as absolute numbers of running machines or as a percentage of machines in the desktop group that are to be maintained as running.

A value of $true indicates that the pool size array values are percentages of total machines in the desktop group and a value of $false indicates that the pool size array values are absolute numbers of machines to maintain as running.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.PowerTimeScheme The power time scheme to be changed.

Return Values

None or Citrix.Broker.Admin.SDK.PowerTimeScheme

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.PowerTimeScheme object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerPowerTimeScheme -Name 'Development Weekdays' -PoolSize ( 0..23 | %{ if ($_ -lt 8 -or $_ -gt 19) { 5 } else { 20 } } )
```

Sets the pool size for the power time scheme named 'Development Weekdays' to be 20 for the time between 8am to 7:59pm, and 5 for other times.

Set-BrokerPowerTimeSchemeMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for PowerTimeScheme

Syntax

Set-BrokerPowerTimeSchemeMetadata [-PowerTimeSchemeId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerPowerTimeSchemeMetadata [-PowerTimeSchemeId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerPowerTimeSchemeMetadata [-PowerTimeSchemeId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerPowerTimeSchemeMetadata [-InputObject] <PowerTimeScheme[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerPowerTimeSchemeMetadata [-InputObject] <PowerTimeScheme[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerPowerTimeSchemeMetadata [-PowerTimeSchemeName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerPowerTimeSchemeMetadata [-PowerTimeSchemeName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerPowerTimeSchemeMetadata cmdlet creates/updates metadata key-value pairs for PowerTimeScheme. The PowerTimeScheme can be specified by InputObject or piping.

Related topics

Parameters

-PowerTimeSchemeId<Int32>

Specifies the PowerTimeScheme object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-InputObject<PowerTimeScheme[]>

Specifies the PowerTimeScheme objects whose Metadata is to be created/updated.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-PowerTimeSchemeName<String>

Specifies the PowerTimeScheme object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerPowerTimeScheme You can pipe the PowerTimeScheme to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerPowerTimeScheme

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerPowerTimeScheme object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerPowerTimeSchemeMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the PowerTimeScheme whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerPowerTimeScheme | Set-BrokerPowerTimeSchemeMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the PowerTimeScheme in the site

---------- EXAMPLE 3 ----------

```
C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerPowerTimeSchemeMetadata 'objname'
```

This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the PowerTimeScheme in the site whose name is 'objname'

Set-BrokerPrivateDesktop

Sep 10, 2014

Change the settings of a private desktop.

Syntax

Set-BrokerPrivateDesktop [-InputObject] <PrivateDesktop[]> [-PassThru] [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-ColorDepth <ColorDepth>] [-Description <String>] [-IconUid <Int32>] [-InMaintenanceMode <Boolean>] [-PublishedName <String>] [-SecureIcaRequired <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerPrivateDesktop [-MachineName] <String> [-PassThru] [-AssignedClientName <String>] [-AssignedIPAddress <String>] [-ColorDepth <ColorDepth>] [-Description <String>] [-IconUid <Int32>] [-InMaintenanceMode <Boolean>] [-PublishedName <String>] [-SecureIcaRequired <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Private desktops are automatically created when a machine is added to a desktop group with a DesktopKind of 'Private', and these inherit default properties. Use Set-BrokerPrivateDesktop to change the configuration settings of an existing private desktop.

To specify private desktops, you can choose whether to update by machine name, or by passing a PrivateDesktop or an array of PrivateDesktop objects. You can also use the Uid or an array of Uids instead.

You cannot modify many properties of a private desktop as these contain status information; for example DNSName, RegistrationState, and OSVersion.

Use Add- and Remove- cmdlets to update relationships between private desktops and other objects. For example, you can add a tag to a private desktop with:

Add-BrokerTag $tag -Desktop $desktop.Uid

Similarly, assign users to private desktops with:

Add-BrokerUser $user -PrivateDesktop $desktop

Many of the fields that can be set with this cmdlet can also be set with Set-BrokerMachine, such as MaintenanceMode. Using Set-BrokerMachine is preferred in these cases.

For more information about desktops, see about_Broker_Desktops; for more information about machines, see about_Broker_Machines.

Related topics

Get-BrokerMachine

Parameters

-InputObject<PrivateDesktop[]>

Specifies the desktop or array of desktops to modify. You can also use an integer Uid of the desktop instead.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-MachineName<String>

Specifies the desktop to modify using its machine name (in the form 'domain\machine').

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-AssignedClientName<String>

Changes the client name assignment of the desktop. Set this to $null to remove the assignment. Desktops can be assigned to multiple users, a single IP address, or a single client name, but only to one of these categories at one time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AssignedIPAddress<String>

Changes the IP address assignment of the desktop. Set this to $null to remove the assignment. Desktops can be assigned to multiple users, a single IP address, or a single client name, but only to one of these categories at one time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Changes the color depth connections to this desktop should use.

Valid values are $null, FourBit, EightBit, SixteenBit, and TwentyFourBit. A value of $null results in the desktop group value being used instead.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Changes the description of the desktop. This is seen only by Citrix Administrators and is not visible to users.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IconUid<Int32>

Changes the icon displayed for this desktop. When this setting is $null, the icon displayed is determined by the desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Changes the maintenance mode setting of a desktop. When a desktop is in maintenance mode, it is not included as a candidate when brokering new sessions, and it does not participate in automatic power management (idle pool); however, it still responds to explicit power operations.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PublishedName<String>

Changes the name displayed to the user for this desktop. When this setting is $null, the name displayed is determined by the PublishedName of the desktop group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Changes whether or not SecureICA is required for connections to this desktop. When this setting is $null, the SecureIcaRequired setting from the desktop group is used.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.PrivateDesktop You can pipe PrivateDesktop objects into this cmdlet instead of on the command line with the -

InputObject parameter.

Return Values

None or Citrix.Broker.Admin.SDK.PrivateDesktop

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.PrivateDesktop object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerPrivateDesktop DOMAIN\Machine1 -ColorDepth SixteenBit
```

Change the color depth of Machine1 to be 16-bit.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerPrivateDesktop -InMaintenanceMode $true | Set-BrokerPrivateDesktop -InMaintenanceMode $false
```

Bring all private desktops currently in maintenance mode back into normal service.

Set-BrokerRebootCycleMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for RebootCycle

Syntax

Set-BrokerRebootCycleMetadata [-RebootCycleId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerRebootCycleMetadata [-RebootCycleId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerRebootCycleMetadata [-RebootCycleId] <Int64> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerRebootCycleMetadata [-InputObject] <RebootCycle[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerRebootCycleMetadata [-InputObject] <RebootCycle[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerRebootCycleMetadata cmdlet creates/updates metadata key-value pairs for RebootCycle. The RebootCycle can be specified by InputObject or piping.

Related topics

Parameters

-RebootCycleId<Int64>

Specifies the RebootCycle object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-InputObject<RebootCycle[]>

Specifies the RebootCycle objects whose Metadata is to be created/updated.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False

Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerRebootCycle You can pipe the RebootCycle to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerRebootCycle

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerRebootCycle object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerRebootCycleMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the RebootCycle whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerRebootCycle | Set-BrokerRebootCycleMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the RebootCycle in the site

Set-BrokerRebootSchedule

Sep 10, 2014

Updates the values of one or more desktop group reboot schedules.

Syntax

```
Set-BrokerRebootSchedule [-InputObject] <RebootSchedule[]> [-PassThru] [-Day <RebootScheduleDays>] [-Enabled <Boolean>] [-Frequency <RebootScheduleFrequency>] [-RebootDuration <Int32>] [-StartTime <TimeSpan>] [-WarningDuration <Int32>] [-WarningMessage <String>] [-WarningTitle <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerRebootSchedule [-DesktopGroupName] <String> [-PassThru] [-Day <RebootScheduleDays>] [-Enabled <Boolean>] [-Frequency <RebootScheduleFrequency>] [-RebootDuration <Int32>] [-StartTime <TimeSpan>] [-WarningDuration <Int32>] [-WarningMessage <String>] [-WarningTitle <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Set-BrokerRebootSchedule cmdlet is used to alter the settings of an existing desktop group reboot schedule.

Related topics

Get-BrokerRebootSchedule

New-BrokerRebootSchedule

Remove-BrokerRebootSchedule

Parameters

-InputObject<RebootSchedule[]>

The reboot schedule to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroupName<String>

The name of the desktop group whose reboot schedule is to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-Day<RebootScheduleDays>

For weekly schedules, the day of the week on which the scheduled reboot-cycle starts (one of Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Boolean that indicates if the reboot schedule is to be enabled or disabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Frequency<RebootScheduleFrequency>

Frequency with which this schedule runs (either Weekly or Daily).

Required?	false
Default Value	
Accept Pipeline Input?	false

-RebootDuration<Int32>

Approximate maximum number of minutes over which the scheduled reboot cycle runs.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartTime<TimeSpan>

Time of day at which the scheduled reboot cycle starts (HH:MM).

Required?	false
Default Value	
Accept Pipeline Input?	false

-WarningDuration<Int32>

Time prior to the initiation of a machine reboot at which warning message is displayed in all user sessions on that machine. If the warning duration is zero then no message is displayed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WarningMessage<String>

Warning message displayed in user sessions on a machine scheduled for reboot. If the message is blank then no message is displayed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WarningTitle<String>

The window title used when showing the warning message in user sessions on a machine scheduled for reboot.

Required?	false
Default Value	

Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.RebootSchedule Reboot schedules may be specified through pipeline input.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerRebootSchedule -DesktopGroupName Accounting -WarningMessage "Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
```

Sets the reboot schedule for the desktop group named Accounting to display a message with the title "WARNING: Reboot pending" and body "Save your work" ten minutes prior to rebooting each machine. The message is displayed in every user session on that machine.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerRebootSchedule -Frequency Weekly | Set-BrokerRebootSchedule -Day Friday
```

Sets all weekly reboot schedules to run on Friday.

Set-BrokerRemotePCAccount

Sep 10, 2014

Modify one or more RemotePCAccounts.

Syntax

Set-BrokerRemotePCAccount [-InputObject] <RemotePCAccount[]> [-PassThru] [-AllowSubfolderMatches <Boolean>] [-MachinesExcluded <String[]>] [-MachinesIncluded <String[]>] [-OU <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Modify one or more RemotePCAccounts.

Related topics

Get-BrokerRemotePCAccount

New-BrokerRemotePCAccount

Remove-BrokerRemotePCAccount

Parameters

-InputObject<RemotePCAccount[]>

Specifies the RemotePCAccounts to modify.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-AllowSubfolderMatches<Boolean>

When true a machine matches this RemotePCAccount if the AD computer is in the container specified by the OU property, or within a child container of the OU.

When false the AD computer object only matches if it is directly in the AD container specified by the OU property.

This property is not meaningful when OU has the special value 'any'.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachinesExcluded<String[]>

MachinesExcluded specifies a set of strings that can include asterisk wildcards. If a machine name matches any entries in MachinesExcluded then it cannot match with this RemotePCAccount regardless of whether there is a MachinesIncluded match.

Matches are performed against the domain name joined with the machine name by a backslash (DOMAIN\MACHINE), e.g.:

DOMAIN1\M*

DOMAIN*\M*

\M

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachinesIncluded<String[]>

MachinesIncluded specifies a set of strings that can include asterisk wildcards. A machine may only match with this RemotePCAccount if it matches a MachinesIncluded entry and does not match any MachinesExcluded entries.

Matches are performed against the domain name joined with the machine name by a backslash (DOMAIN\MACHINE), e.g.:

DOMAIN1\M*

DOMAIN*\M*

\M

Required?	false

Default Value	
Accept Pipeline Input?	false

-OU<String>

Specifies the DN of an AD container, or has the special value 'any'.

When an AD container is specified a machine may only match with the RemotePCAccount when the AD computer object is located relative to the OU.

When 'any' is specified the location of the AD computer object is ignored for purposes of matching this RemotePCAccount. The machine must still meet the MachinesIncluded and MachinesExcluded filters for a match to occur.

In the event that a machine matches with multiple RemotePCAccounts then the RemotePCAccount OU with the longest canonical name takes precedence. The special 'any' OU is treated as lowest priority.

Note that the OU value of every RemotePCAccount must be unique, and this includes only one 'any' entry being permitted.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.RemotePCAccount You can pipe the RemotePCAccounts to be modified into this cmdlet.

Return Values

None or Citrix.Broker.Admin.SDK.RemotePCAccount

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.RemotePCAccount object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerRemotePCAccount | Set-BrokerRemotePCAccount -MachinesExcluded @('DOMAIN42*')
Make all RemotePCAccounts filter out machines from DOMAIN42.

Set-BrokerSession

Sep 10, 2014

Sets properties of a session.

Syntax

```
Set-BrokerSession [-InputObject] <Session[]> [-PassThru] [-Hidden <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSession [-SessionKey] <Guid> [-PassThru] [-Hidden <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Set-BrokerSession cmdlet sets properties on a session or set of sessions. You can specify a single session by Uid or SessionKey (Guid) or multiple session instances can be passed to the command by piping or using the -InputObject parameter.

Related topics

Get-BrokerSession

Parameters

-InputObject<Session[]>

The session instances whose properties you want to set.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-SessionKey<Guid>

The session key (Guid) of the session whose properties you want to set.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-Hidden<Boolean>

Changes whether the session is hidden or not. Hidden sessions are treated as though they do not exist when brokering sessions; a hidden session cannot be reconnected to, but a new session may be launched using the same entitlement.

A session may be hidden automatically by the system when an attempt is made to reconnect to a session that is unreachable due to, for example, the failure of a VM's hypervisor. This allows a new session to be brokered provided that other machines in the same desktop group are still available. If the original session still exists after the hypervisor is restored then it must be unhidden to allow the user to reconnect to it.

Only sessions for shared desktops or applications can be hidden or unhidden. Private desktop or application sessions can never be hidden.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host

name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Session You can pipe in the sessions whose properties you want to set.

Return Values

None or Citrix.Broker.Admin.SDK.Session

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.Session object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $sessions = Get-BrokerSession -User ACCOUNTS\JohnSmith -Hidden $true
C:\PS> $sessions | Set-BrokerSession -Hidden $false
```

Finds all sessions in the site for user John Smith that have been hidden, and makes them available for reconection again.

Set-BrokerSessionLinger

Sep 10, 2014

Updates the values of one or more desktop group session linger settings.

Syntax

```
Set-BrokerSessionLinger [-InputObject] <SessionLinger[]> [-PassThru] [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Set-BrokerSessionLinger [-DesktopGroupName] <String> [-PassThru] [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Set-BrokerSessionLinger cmdlet is used to alter the settings of an existing desktop group session linger setting.

Related topics

New-BrokerSessionLinger

Get-BrokerSessionLinger

Remove-BrokerSessionLinger

Parameters

-InputObject<SessionLinger[]>

The session linger to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroupName<String>

The name of the desktop group whose session linger setting is to be modified.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-Enabled<Boolean>

Boolean that indicates if the session linger setting is to be enabled or disabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxAverageLoadThreshold<Int32>

Specifies the average load threshold across the desktop group. When the threshold hits, lingering sessions across the group be terminated to reduce load. Sessions that have been lingering the longest will be chosen first.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxLoadPerMachineThreshold<Int32>

Specifies the maximum load threshold per machine in the desktop group. When the threshold hits, lingering sessions on each loaded machine will be terminated to reduce load. Sessions that have been lingering the longest will be chosen first.

Required?	false

Default Value	
Accept Pipeline Input?	false

-MaxTimeBeforeDisconnect<TimeSpan>

Specifies the time by which a lingering session will be disconnected. The disconnect time cannot be greater than the terminate timer (if enabled). When the disconnect and terminate times are the same, the terminate time takes precedence.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxTimeBeforeTerminate<TimeSpan>

Specifies the time by which a lingering session will be terminated. When the disconnect and terminate times are the same, the terminate time takes precedence.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserFilterEnabled<Boolean>

Specifies whether the session linger's user filter is enabled or disabled. Where the user filter is enabled, lingering is enabled only to users who appear in the filter (either explicitly or by virtue of group membership).

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.SessionLinger Session linger settings may be specified through pipeline input.

Return Values

None or Citrix.Broker.Admin.SDK.SessionLinger

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.SessionLinger object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerSessionLinger -DesktopGroupName Accounting -MaxTimeBeforeDisconnect 0:10
```

Sets the disconnect time for the session linger setting associated with desktop group named Accounting.

Set-BrokerSessionMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for Session

Syntax

Set-BrokerSessionMetadata [-SessionId] <Int64> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSessionMetadata [-SessionId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSessionMetadata [-SessionId] <Int64> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSessionMetadata [-InputObject] <Session[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSessionMetadata [-InputObject] <Session[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSessionMetadata [-SessionName] <Guid> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSessionMetadata [-SessionName] <Guid> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerSessionMetadata cmdlet creates/updates metadata key-value pairs for Session. The Session can be specified by InputObject or piping.

Related topics

Parameters

-SessionId<Int64>

Specifies the Session object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Session[]>

Specifies the Session objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-SessionName<Guid>

Specifies the Session object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerSession You can pipe the Session to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerSession

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerSession object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerSessionMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the Session whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerSession | Set-BrokerSessionMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the Session in the site

---------- EXAMPLE 3 ----------

C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerSessionMetadata 'objname'
This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the Session in the site whose name is 'objname'

Set-BrokerSessionPreLaunch

Sep 10, 2014

Updates the values of one or more desktop group session pre-launch settings.

Syntax

```
Set-BrokerSessionPreLaunch [-InputObject] <SessionPreLaunch[]> [-PassThru] [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Set-BrokerSessionPreLaunch [-DesktopGroupName] <String> [-PassThru] [-Enabled <Boolean>] [-MaxAverageLoadThreshold <Int32>] [-MaxLoadPerMachineThreshold <Int32>] [-MaxTimeBeforeDisconnect <TimeSpan>] [-MaxTimeBeforeTerminate <TimeSpan>] [-UserFilterEnabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Set-BrokerSessionPreLaunch cmdlet is used to alter the settings of an existing desktop group session pre-launch setting.

Related topics

New-BrokerSessionPreLaunch

Get-BrokerSessionPreLaunch

Remove-BrokerSessionPreLaunch

Parameters

-InputObject<SessionPreLaunch[]>

The session pre-launch to be modified.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-DesktopGroupName<String>

The name of the desktop group whose session pre-launch setting is to be modified.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-Enabled<Boolean>

Boolean that indicates if the session pre-launch setting is to be enabled or disabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxAverageLoadThreshold<Int32>

Specifies the average load threshold across the desktop group. When the threshold hits, pre-launched sessions across the group be terminated to reduce load. Sessions that have been pre-launched the longest will be chosen first.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxLoadPerMachineThreshold<Int32>

Specifies the maximum load threshold per machine in the desktop group. When the threshold hits, pre-launched sessions on each loaded machine will be terminated to reduce load. Sessions that have been pre-launched the longest will be chosen first.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxTimeBeforeDisconnect<TimeSpan>

Specifies the time by which a pre-launched session will be disconnected. The disconnect time cannot be greater than the terminate timer (if enabled). When the disconnect and terminate times are the same, the terminate time takes precedence.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxTimeBeforeTerminate<TimeSpan>

Specifies the time by which a pre-launched session will be terminated. When the disconnect and terminate times are the same, the terminate time takes precedence.

Required?	false
Default Value	
Accept Pipeline Input?	false

-UserFilterEnabled<Boolean>

Specifies whether the session pre-launch's user filter is enabled or disabled. Where the user filter is enabled, pre-launch is enabled only to users who appear in the filter (either explicitly or by virtue of group membership).

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop

Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.SessionPreLaunch Session pre-launch settings may be specified through pipeline input.

Return Values

None or Citrix.Broker.Admin.SDK.SessionPreLaunch

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.SessionPreLaunch object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerSessionPreLaunch -DesktopGroupName Accounting -MaxTimeBeforeDisconnect 0:10
Sets the disconnect time for the session pre-launch setting associated with desktop group named Accounting.

Set-BrokerSharedDesktop

Sep 10, 2014

Change the settings of a shared desktop.

Syntax

```
Set-BrokerSharedDesktop [-InputObject] <SharedDesktop[]> [-PassThru] [-InMaintenanceMode <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSharedDesktop [-MachineName] <String> [-PassThru] [-InMaintenanceMode <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Shared desktops are automatically created when a machine is added to a desktop group with a DesktopKind of 'Shared', and these inherit default properties. Use Set-BrokerSharedDesktop to change the configuration settings of an existing shared desktop.

To specify shared desktops, you can choose whether to update by machine name or by passing a SharedDesktop or an array of SharedDesktop objects. You can also use the Uid or an array of Uids instead.

Most properties of a shared desktop cannot be modified as these contain status information; for example DNSName, RegistrationState, and OSVersion. You can change only the maintenance mode setting with this cmdlet.

Many of the properties that can be set with Set-BrokerSharedDesktop can be set by using Set-BrokerMachine (e.g. InMaintenanceMode). Using the Set-BrokerMachine cmdlet, where possible, is the preferred behaviour.

See about_Broker_Desktops for more information about desktops.

Related topics

Get-BrokerSharedDesktop

Parameters

-InputObject<SharedDesktop[]>

Specifies the desktop or array of desktops to modify. You can also use an integer Uid of the desktop instead.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MachineName<String>

Specifies the desktop to modify using its machine name (in the form 'domain\machine').

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-InMaintenanceMode<Boolean>

Changes the maintenance mode setting of a desktop. When a desktop is in maintenance mode, it is not included as a candidate when brokering new sessions, and it does not participate in automatic power management (idle pool); however, it still responds to explicit power operations.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.SharedDesktop You can pipe SharedDesktop objects into this cmdlet instead of on the command line with the -InputObject parameter.

Return Values

None or Citrix.Broker.Admin.SDK.SharedDesktop

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.SharedDesktop object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerSharedDesktop DOMAIN\Machine1 -InMaintenanceMode $true
```

Put the Machine1 shared desktop into maintenance mode.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerSharedDesktop -InMaintenanceMode $true | Set-BrokerSharedDesktop -InMaintenanceMode $false
```

Bring all shared desktops currently in maintenance mode back into normal service.

Set-BrokerSite

Sep 10, 2014

Changes the overall settings of the current XenDesktop broker site.

Syntax

```
Set-BrokerSite [-PassThru] [-BaseOU <Guid>] [-ColorDepth <ColorDepth>] [-ConnectionLeasingEnabled <Boolean>] [-DesktopGroupIconUid <Int32>] [-DnsResolutionEnabled <Boolean>] [-SecureIcaRequired <Boolean>] [-TrustRequestsSentToTheXmlServicePort <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Set-BrokerSite cmdlet modifies properties of the current broker site.

The broker site is a top-level, logical representation of the XenDesktop site, from the perspective of the brokering services running within the site. It defines various site-wide default attributes used by the brokering services.

A XenDesktop installation has only a single broker site instance.

Related topics

Get-BrokerSite

New-BrokerIcon

Parameters

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-BaseOU<Guid>

Changes the objectGUID property identifying the base OU in Active Directory used for desktop registrations. For sites using only registry-based discovery (the default) this value is $null.

Any desktop attempting to register through a different OU from the one specified here is rejected. Note that desktops configured for registry-based discovery can register with the site, even if a BaseOU value is specified.

Information held in Active Directory is not modified by changing this value.

Typically, this property is changed only by using the Set-ADControllerDiscovery.ps1 script.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ColorDepth<ColorDepth>

Changes the default color depth for new desktop groups, if no color depth is specified explicitly when a group is created. Changing this default has no impact on the color depths used already by existing groups.

Valid values are FourBit, EightBit, SixteenBit, and TwentyFourBit.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ConnectionLeasingEnabled<Boolean>

Enabled or disable connection leasing on the site.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DesktopGroupIconUid<Int32>

Changes the default desktop icon used for new desktop groups if no icon is specified explicitly when a group is created. Changing this default has no impact on the icons used already by existing groups.

The specified icon must already have been added to the site using New-BrokerIcon.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DnsResolutionEnabled<Boolean>

Changes whether ICA files returned by a broker service to a user device contain the numeric IP address or the DNS name of the desktop machine to which a session should be established.

With the default value ($false), ICA files will always contain a numeric IP address. To have DNS names appear in the ICA files, set the value to $true.

Even when DNS resolution is enabled ($true), IP addresses may still appear in ICA files. The reasons for this include, for example, that the broker service is unable to obtain a DNS name for the target machine, or that Web Interface is configured to always use numeric IP addresses in this context.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecureIcaRequired<Boolean>

Changes the default SecureICA usage requirements for new desktop groups if no SecureICA setting is specified explicitly when a group is created. Changing this default has no impact on the SecureICA usage requirements of existing groups.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TrustRequestsSentToTheXmlServicePort<Boolean>

Changes whether the XML Service (as used by Web Interface) implicitly trusts the originator of requests it receives, or whether it fully authenticates them.

With the default value ($false), full authentication checks are performed. However, you must enable this setting ($true) to allow support for "Pass-through" authentication, and/or connections routed through Access Gateway.

If this setting is enabled, you must ensure that controllers running the brokering services are securely firewalled.

Required?	false
Default Value	

Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

None or Citrix.Broker.Admin.SDK.Site

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.Site object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerSite -ColorDepth SixteenBit

Specifies that any new desktop groups created, where a color depth value is not specified, default to using 16-bit color depth for user sessions to desktops or applications within that group.

Set-BrokerSiteMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for Site

Syntax

Set-BrokerSiteMetadata -Name <String> -Value <String> [[-InputObject] <Site[]>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSiteMetadata -Map <PSObject> [[-InputObject] <Site[]>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSiteMetadata -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSiteMetadata -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerSiteMetadata -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerSiteMetadata cmdlet creates/updates metadata key-value pairs for Site. The Site can be specified by InputObject or piping.

Related topics

Parameters

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-InputObject<Site[]>

Specifies the Site objects whose Metadata is to be created/updated.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerSite You can pipe the Site to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerSite

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerSite object.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-BrokerSiteMetadata -Name "MyMetadataName" -Value "1234"
```
This command creates/updates the Metadata "MyMetadataName" key-value pair for the Site

---------- EXAMPLE 2 ----------

```
C:\PS> Get-BrokerSite | Set-BrokerSiteMetadata -Name "MyMetadataName" -Value "1234"
```
This command creates/updates metadata key "MyMetadataName" with the value "1234"

Set-BrokerTagMetadata

Sep 10, 2014

Creates/Updates metadata key-value pairs for Tag

Syntax

Set-BrokerTagMetadata [-TagId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerTagMetadata [-TagId] <Int32> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerTagMetadata [-TagId] <Int32> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerTagMetadata [-InputObject] <Tag[]> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerTagMetadata [-InputObject] <Tag[]> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerTagMetadata [-TagName] <String> -Map <PSObject> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-BrokerTagMetadata [-TagName] <String> -Name <String> -Value <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-BrokerTagMetadata cmdlet creates/updates metadata key-value pairs for Tag. The Tag can be specified by InputObject or piping.

Related topics

Parameters

-TagId<Int32>

Specifies the Tag object whose Metadata is to be created/updated by ID.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-InputObject<Tag[]>

Specifies the Tag objects whose Metadata is to be created/updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-TagName<String>

Specifies the Tag object whose Metadata is to be created/updated by name.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Name<String>

Specifies the name of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Value<String>

Specifies the value of the Metadata member to be created/updated

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a hashtable containing name/value pairs to be used to create or update Metadata members

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-PassThru<SwitchParameter>

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it returns the affected record.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.BrokerTag You can pipe the Tag to hold the new or updated metadata.

Return Values

None or Citrix.Broker.Admin.SDK.BrokerTag

This cmdlet does not generate any output, unless you use the PassThru parameter, in which case it generates a Citrix.Broker.Admin.SDK.BrokerTag object.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-BrokerTagMetadata -InputObject $obj-Uid -Name "MyMetadataName" -Value "1234"
This command creates/updates the Metadata "MyMetadataName" key-value pair for the Tag whose instance is pointed by $obj-Uid

---------- EXAMPLE 2 ----------

C:\PS> Get-BrokerTag | Set-BrokerTagMetadata -Name "MyMetadataName" -Value "1234"
This command creates/updates metadata key "MyMetadataName" with the value "1234" for all the Tag in the site

---------- EXAMPLE 3 ----------

C:\PS> @{ 'name1' = 'value1'; 'name2' = 'value2' } | Set-BrokerTagMetadata 'objname'
This command creates/updates two metadata keys "name1" and "name2" with the values "value1" and "value2" respectively for the Tag in the site whose name is 'objname'

Start-BrokerCatalogPvdImagePrepare

Sep 10, 2014

Start the PVD Image prepare process in the Broker for the machines in the specified catalog(s).

Syntax

Start-BrokerCatalogPvdImagePrepare [-InputObject] <Catalog[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Start-BrokerCatalogPvdImagePrepare cmdlet instructs the Broker to request the Personal VDisk (PVD) preparation process for all of the machines in the specified catalog(s). The process begins when each machine is subsequently powered off, at which point brokering of user desktop sessions is suspended as well as regular machine power operations until the process completes. Only catalogs with a PersistUserChanges value of OnPvd are supported by this cmdlet.

Related topics

Start-BrokerMachinePvdImagePrepare

Parameters

-InputObject<Catalog[]>

The catalog(s) holding the machines on which to start the PVD Image Preparation process.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Catalog You can pipe in the catalogs on which to start the PVD image preparation process.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerCatalog 'MyCatalog' | Start-BrokerCatalogPvdImagePrepare
```

Instruct the Broker that the Personal VDisk preparation process will start the next time the machines in the specified catalog are powered off.

Start-BrokerMachinePvdImagePrepare

Sep 10, 2014

Start the PVD Image prepare process in the Broker for the specified machine(s).

Syntax

Start-BrokerMachinePvdImagePrepare [-InputObject] <Machine[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Start-BrokerMachinePvdImagePrepare cmdlet instructs the Broker to request the Personal VDisk (PVD) preparation process for the specified machine(s). The process begins when each machine is subsequently powered off, at which point brokering of user desktop sessions is suspended as well as regular machine power operations until the process completes. Only machines in catalogs with a PersistUserChanges value of OnPvd are supported by this cmdlet.

Related topics

Start-BrokerCatalogPvdImagePrepare

Parameters

-InputObject<Machine[]>

The machine(s) to start the PVD Image Preparation process on.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Machine You can pipe in the machines to start the PVD image preparation process on.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerMachine 'MyMachine' | Start-BrokerMachinePvdImagePrepare
Instruct the Broker that the Personal VDisk preparation process will start the next time the specified machine(s) are powered off.

Start-BrokerNaturalRebootCycle

Sep 10, 2014

Reboots all machines from the specified catalog when they are not in use.

Syntax

```
Start-BrokerNaturalRebootCycle [-InputObject] <Catalog[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Creating a natural reboot cycle for catalog ensures that all machines in the catalog are running the most recent image for the catalog and that all PvD image updates have been performed.

The machines are rebooted in a non disruptive manner, allowing machines that are in use to continue working and be restarted only after they become idle.

Related topics

None

Parameters

-InputObject<Catalog[]>

Reboots all machines from this input catalog. The catalogs can be specified using UID values, name values (including wildcards) or catalog objects.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Catalog Catalogs may be specified through pipeline input. The catalogs can be specified using UID values, name values (including wildcards) or catalog objects

Return Values

None

Notes

Natural reboot cycles do not apply to non-power managed and multi session catalogs

Examples

---------- EXAMPLE 1 ----------

```
$c = Get-BrokerCatalog -Uid 1
    Start-BrokerNaturalRebootCycle -InputObject $c
```

The above code applies a natural reboot cycle on catalog with Id 1

Start-BrokerRebootCycle

Sep 10, 2014

Creates and starts a reboot cycle for each desktop group that contains machines from the specified catalog.

Syntax

```
Start-BrokerRebootCycle [-InputObject] <Catalog[]> -RebootDuration <Int32> [-WarningDuration <Int32>] [-WarningTitle <String>] [-WarningMessage <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Start-BrokerRebootCycle cmdlet is used to create and start a reboot cycle for each desktop group that contains machines from the specified catalog. For a given desktop group, only the machines from the target catalog are rebooted and any machines from other catalogs are not rebooted.

Creating a reboot cycle for catalog ensures that all machines in the catalog are running the most recent image for the catalog and that all PvD image updates have been performed.

Related topics

Stop-BrokerRebootCycle

Get-BrokerRebootCycle

Parameters

-InputObject<Catalog[]>

Creates a reboot cycle for each desktop group that contains machines from this input catalog SDK object. The catalogs can be specified using UID values, name values (including wildcards) or catalog objects.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-RebootDuration<Int32>

Approximate maximum duration in minutes over which the reboot cycle runs.

Required?	true
Default Value	
Accept Pipeline Input?	false

-WarningDuration<Int32>

Time in minutes prior to a machine reboot at which a warning message is displayed in all user sessions on that machine. If the warning duration value is zero then no message is displayed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WarningTitle<String>

The window title used when showing the warning message in user sessions on a machine scheduled for reboot.

Required?	false
Default Value	
Accept Pipeline Input?	false

-WarningMessage<String>

Warning message displayed in user sessions on a machine scheduled for reboot. If the message is blank then no message is displayed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Catalog Catalogs may be specified through pipeline input. The catalogs can be specified using UID values, name values (including wildcards) or catalog objects

Return Values

none

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerCatalog -Name "SampleCatalog" | Start-BrokerRebootCycle -RebootDuration 240 -WarningMessage "Save your work" -WarningDuration 15
Starts a new reboot cycle for each desktop group containing machines from the catalog "SampleCatalog". Each reboot cycle will have a duration of six hours. Fifteen minutes prior to rebooting a machine, the message "Save your work" will be displayed in each active user session.

Stop-BrokerRebootCycle

Sep 10, 2014

Cancels the specified reboot cycle.

Syntax

```
Stop-BrokerRebootCycle [-InputObject] <RebootCycle[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Stop-BrokerRebootCycle cmdlet is used to cancel the specified reboot cycle.

Related topics

Get-BrokerRebootCycle

Start-BrokerRebootCycle

Parameters

-InputObject<RebootCycle[]>

Cancels this reboot cycle.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host

name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.RebootCycle Reboot cycles may be specified through pipeline input.

Return Values

none

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-BrokerRebootCycle -CatalogUid 7 | Stop-BrokerRebootCycle
Cancels every reboot cycle for the catalog that has the Uid of 7.

Stop-BrokerSession

Sep 10, 2014

Stop or log off a session.

Syntax

```
Stop-BrokerSession [-InputObject] <Session[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Stops or logs off sessions.

Related topics

Disconnect-BrokerSession

Get-BrokerSession

Parameters

-InputObject<Session[]>

Identifies the session(s) to terminate. This can be expressed as either a session Uid or a session object.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Citrix.Broker.Admin.SDK.Session The sessions to stop can be piped into this cmdlet.

Return Values

None

Notes

This operation is non-blocking and returns before it completes. The operation, however, is unlikely to fail unless there are communication problems between the controller and the machine, if bad arguments are passed to the cmdlet itself or if the machine cannot successfully execute the operation.

The transient nature of sessions means that the list of session objects or UIDs supplied to Stop-BrokerSession could consist of valid and invalid sessions. Invalid sessions are detected and disregarded and the stop session operation is invoked on the valid sessions.

The system can fail to invoke the operation if the machine is not in an appropriate state or if there are problems in communicating with the machine. When an operation is invoked the system detects if the operation was initiated successfully or not by the machine. As this operation is non-blocking the system doesn't detect or report whether the operation ultimately succeeded or failed after its successful initialization on the machine.

Operation failures are reported through the broker SDK error handling mechanism (see about_Broker_ErrorHandling). In the event of errors the SdkErrorRecord error status is set to SessionOperationFailed and its error data dictionary is populated with the following entries:

o OperationsAttemptedCount - The number of operations attempted.

o OperationsFailedCount - The number of failed operations.

o OperationsSucceededCount - The number of successfully executed operations.

o UnresolvedSessionFailuresCount - The number of operations that failed due to invalid sessions being supplied.

o OperationInvocationFailuresCount - The number of operations that failed because they could not be invoked on the desktop.

o DesktopExecutionFailuresCount - The number of operations that failed because they could not be successfully executed by the desktop.

The SdkErrorRecord message will also display the number of attempted, failed and successful operations in the following format:

"Session operation error - attempted:<OperationsAttemptedCount>, failed:<OperationsFailedCount>, succeeded:<OperationsSucceededCount>"

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-BrokerSession -UserName MyDomain\MyAccount | Stop-BrokerSession
```
Stops all sessions for the user MyDomain\MyAccount.

---------- EXAMPLE 2 ----------

```
C:\PS> $desktop = Get-BrokerDesktop -DNSName MyMachine.MyDomain.com
C:\PS> Stop-BrokerSession $desktop.SessionUid
```
Stops the session on MyMachine.

---------- EXAMPLE 3 ----------

```
C:\PS> Get-BrokerSession -Filter { SessionState -eq 'Disconnected' -and SessionStateChangeTime -lt '-1' } | Stop-BrokerSession
```
Stop sessions that have been disconnected for more than one day.

---------- EXAMPLE 4 ----------

```
C:\PS> trap  [Citrix.Broker.Admin.SDK.SdkOperationException]
C:\PS> {
C:\PS>   write $("Exception name = " + $_.Exception.GetType().FullName)
C:\PS>   write $("SdkOperationException.Status = " + $_.Exception.Status)
C:\PS>   write $("SdkOperationException.ErrorData=")
C:\PS>   $_.Exception.ErrorData
```

```
C:\PS>
C:\PS>   write $("SdkOperationException.InnerException = " + $_.Exception.InnerException)
C:\PS>   $_.Exception.InnerException
C:\PS>   continue
C:\PS> }
C:\PS>
C:\PS> Stop-BrokerSession -InputObject 10,11,12
```

Trap and display error information.

Test-BrokerAccessPolicyRuleNameAvailable

Sep 10, 2014

Determine whether the proposed AccessPolicyRule Name is available for use.

Syntax

```
Test-BrokerAccessPolicyRuleNameAvailable [-Name] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed AccessPolicyRule Name is available for use. It returns a record for each Name indicating the availability of that Name, with $true indicating that the Name is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerAccessPolicyRule

New-BrokerAccessPolicyRule

Rename-BrokerAccessPolicyRule

Parameters

-Name<String[]>

The AccessPolicyRule Name to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the Name to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each Name specified. An availability of "True" indicates the Name is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerAccessPolicyRuleNameAvailable -Name Test1
```

Checks whether the Name "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerAccessPolicyRuleNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerAppAssignmentPolicyRuleNameAvailable

Sep 10, 2014

Determine whether the proposed AppAssignmentPolicyRule Name is available for use.

Syntax

```
Test-BrokerAppAssignmentPolicyRuleNameAvailable [-Name] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed AppAssignmentPolicyRule Name is available for use. It returns a record for each Name indicating the availability of that Name, with $true indicating that the Name is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerAppAssignmentPolicyRule

New-BrokerAppAssignmentPolicyRule

Rename-BrokerAppAssignmentPolicyRule

Parameters

-Name<String[]>

The AppAssignmentPolicyRule Name to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the Name to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each Name specified. An availability of "True" indicates the Name is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerAppAssignmentPolicyRuleNameAvailable -Name Test1
```

Checks whether the Name "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerAppAssignmentPolicyRuleNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerAppEntitlementPolicyRuleNameAvailable

Sep 10, 2014

Determine whether the proposed AppEntitlementPolicyRule Name is available for use.

Syntax

```
Test-BrokerAppEntitlementPolicyRuleNameAvailable [-Name] <String[]> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed AppEntitlementPolicyRule Name is available for use. It returns a record for each Name indicating the availability of that Name, with $true indicating that the Name is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerAppEntitlementPolicyRule

New-BrokerAppEntitlementPolicyRule

Rename-BrokerAppEntitlementPolicyRule

Parameters

-Name<String[]>

The AppEntitlementPolicyRule Name to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the Name to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each Name specified. An availability of "True" indicates the Name is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerAppEntitlementPolicyRuleNameAvailable -Name Test1
```

Checks whether the Name "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerAppEntitlementPolicyRuleNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerApplicationNameAvailable

Sep 10, 2014

Determine whether the proposed Application Name is available for use.

Syntax

```
Test-BrokerApplicationNameAvailable [-Name] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed Application Name is available for use. It returns a record for each Name indicating the availability of that Name, with $true indicating that the Name is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerApplication

New-BrokerApplication

Rename-BrokerApplication

Parameters

-Name<String[]>

The Application Name to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the Name to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each Name specified. An availability of "True" indicates the Name is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerApplicationNameAvailable -Name Test1
```

Checks whether the Name "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerApplicationNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerAssignmentPolicyRuleNameAvailable

Sep 10, 2014

Determine whether the proposed AssignmentPolicyRule Name is available for use.

Syntax

```
Test-BrokerAssignmentPolicyRuleNameAvailable [-Name] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed AssignmentPolicyRule Name is available for use. It returns a record for each Name indicating the availability of that Name, with $true indicating that the Name is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerAssignmentPolicyRule

New-BrokerAssignmentPolicyRule

Rename-BrokerAssignmentPolicyRule

Parameters

-Name<String[]>

The AssignmentPolicyRule Name to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the Name to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each Name specified. An availability of "True" indicates the Name is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerAssignmentPolicyRuleNameAvailable -Name Test1
```

Checks whether the Name "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerAssignmentPolicyRuleNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerCatalogNameAvailable

Sep 10, 2014

Determine whether the proposed Catalog Name is available for use.

Syntax

```
Test-BrokerCatalogNameAvailable [-Name] <String[]> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed Catalog Name is available for use. It returns a record for each Name indicating the availability of that Name, with $true indicating that the Name is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerCatalog

New-BrokerCatalog

Rename-BrokerCatalog

Parameters

-Name<String[]>

The Catalog Name to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the Name to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each Name specified. An availability of "True" indicates the Name is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerCatalogNameAvailable -Name Test1
```

Checks whether the Name "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerCatalogNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerDBConnection

Sep 10, 2014

Tests whether a database is suitable for use by the Citrix Broker Service.

Syntax

```
Test-BrokerDBConnection [-DBConnection] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Tests whether the database specified in the given connection string is suitable for use by the currently selected Citrix Broker Service instance.

The service attempts to contact the specified database and returns a status indicating whether the database is both contactable and usable. The test does not impact any currently established connection from the service instance to another database in any way. The tested connection string is not recorded.

Only use of Windows authentication within the connection string is supported; a connection string containing SQL authentication credentials is always rejected as invalid.

The current service instance is the one on the local machine, or the one most recently specified using the -AdminAddress parameter of a Broker SDK cmdlet.

Related topics

Get-BrokerServiceStatus

Get-BrokerDBConnection

Set-BrokerDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the currently selected Citrix Broker Service instance.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-BrokerDBConnection cmdlet returns an object describing the status of the selected Broker Service instance that would result if the connection string were used with the Set-BrokerDBConnection cmdlet together with extra diagnostics information for the specified connection string. The actual current status of the service is not changed. Possible diagnostic values are:

-- OK:

The Set-BrokerDBConnection command would succeed if it were executed with the supplied connection string.

-- DBUnconfigured:

No database connection string is set for the service instance.

-- DBRejectedConnection:

The database rejected the logon attempt from the Broker Service instance. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

-- InvalidDBConfigured:

The specified database does not exist, is not visible to the Broker Service instance, or the service's schema within the database is invalid.

-- DBNotFound:

The specified database could not be located with the given connection string.

-- DBNewerVersionThanService:

The Broker Service instance is older than, and incompatible with, the service's schema in the database. The service instance needs upgrading.

-- DBOlderVersionThanService:

The Broker Service instance is newer than, and incompatible with, the service's schema in the database. The database schema needs upgrading.

-- DBVersionChangeInProgress:

A database schema upgrade is currently in progress.

-- PendingFailure:

Connectivity between the Broker Service instance and the database has been lost. This may be a transitory network error, but may indicate a loss of connectivity that requires administrator intervention.

-- Failed:

Connectivity between the Broker Service instance and the database has been lost for an extended period of time, or has failed due to a configuration problem. The service instance cannot operate while its connection to the database is unavailable.

-- Unknown:

Service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

C:\PS>Test-BrokerDBConnection "Server=dbserver\SQLEXPRESS;Database=XDDB;Trusted_Connection=True"
Tests whether the service instance could use a database called XDDB on an SQL Server Express database running on the machine called dbserver. Integrated Windows authentication is required.

Test-BrokerDesktopGroupNameAvailable

Sep 10, 2014

Determine whether the proposed DesktopGroup Name is available for use.

Syntax

```
Test-BrokerDesktopGroupNameAvailable [-Name] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed DesktopGroup Name is available for use. It returns a record for each Name indicating the availability of that Name, with $true indicating that the Name is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerDesktopGroup

New-BrokerDesktopGroup

Rename-BrokerDesktopGroup

Parameters

-Name<String[]>

The DesktopGroup Name to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the Name to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each Name specified. An availability of "True" indicates the Name is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerDesktopGroupNameAvailable -Name Test1
```

Checks whether the Name "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerDesktopGroupNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerEntitlementPolicyRuleNameAvailable

Sep 10, 2014

Determine whether the proposed EntitlementPolicyRule Name is available for use.

Syntax

```
Test-BrokerEntitlementPolicyRuleNameAvailable [-Name] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed EntitlementPolicyRule Name is available for use. It returns a record for each Name indicating the availability of that Name, with $true indicating that the Name is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerEntitlementPolicyRule

New-BrokerEntitlementPolicyRule

Rename-BrokerEntitlementPolicyRule

Parameters

-Name<String[]>

The EntitlementPolicyRule Name to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the Name to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each Name specified. An availability of "True" indicates the Name is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerEntitlementPolicyRuleNameAvailable -Name Test1
```

Checks whether the Name "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerEntitlementPolicyRuleNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerLicenseServer

Sep 10, 2014

Tests whether or not a license server can be used by the broker.

Syntax

```
Test-BrokerLicenseServer [-ComputerName] <String> [-AdminAddress <String>] [[-Port] <Int32>]
[<CommonParameters>]
```

Detailed Description

Tests whether or not a given license server can be used by the broker.

Related topics

Get-BrokerSite

Set-BrokerSite

Parameters

-ComputerName<String>

The name of the license server to test (machine.domain).

Required?	true
Default Value	None
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

-Port<Int32>

The port number to use on the server.

Required?	false
Default Value	27000
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

System.string

Test-BrokerLicenseServer returns:

o 'Compatible' - the server is a compatible license server that can be used.

o 'Incompatible' - the server is an incompatible license server that can't be used.

o 'Inaccessible' - the server cannot be accessed. The server may be down, unreachable, or non-existent.

o 'InternalError - the server can't be used due to an internal error. A required licensing component on the server may not be installed, configured, or working correctly.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerLicenseServer -LicenseServerAddress "machine.domain" 1234
```

Tests whether or not the license server "machine.domain" with port number 1234 can be used.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerLicenseServer -LicenseServerAddress "machine.domain"
```

Tests whether or not the license server "machine.domain" with port number 2700 can be used.

Test-BrokerMachineNameAvailable

Sep 10, 2014

Determine whether the proposed Machine MachineName is available for use.

Syntax

```
Test-BrokerMachineNameAvailable [-MachineName] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed Machine MachineName is available for use. It returns a record for each MachineName indicating the availability of that MachineName, with $true indicating that the MachineName is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerMachine

New-BrokerMachine

Parameters

-MachineName<String[]>

The Machine MachineName to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the MachineName to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each MachineName specified. An availability of "True" indicates the MachineName is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerMachineNameAvailable -MachineName Test1
```

Checks whether the MachineName "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerMachineNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerPowerTimeSchemeNameAvailable

Sep 10, 2014

Determine whether the proposed PowerTimeScheme Name is available for use.

Syntax

```
Test-BrokerPowerTimeSchemeNameAvailable [-Name] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed PowerTimeScheme Name is available for use. It returns a record for each Name indicating the availability of that Name, with $true indicating that the Name is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerPowerTimeScheme

New-BrokerPowerTimeScheme

Rename-BrokerPowerTimeScheme

Parameters

-Name<String[]>

The PowerTimeScheme Name to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the Name to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each Name specified. An availability of "True" indicates the Name is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerPowerTimeSchemeNameAvailable -Name Test1
```

Checks whether the Name "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerPowerTimeSchemeNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Test-BrokerRemotePCAccountNameAvailable

Sep 10, 2014

Determine whether the proposed RemotePCAccount OU is available for use.

Syntax

```
Test-BrokerRemotePCAccountNameAvailable [-OU] <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This cmdlet checks whether proposed RemotePCAccount OU is available for use. It returns a record for each OU indicating the availability of that OU, with $true indicating that the OU is unused and available for use, or $false if it is not available.

Related topics

Get-BrokerRemotePCAccount

New-BrokerRemotePCAccount

Parameters

-OU<String[]>

The RemotePCAccount OU to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.String You can pipe a string that contains the OU to test.

Return Values

Citrix.Broker.Admin.SDK.NameAvailability

The cmdlet returns a result for each OU specified. An availability of "True" indicates the OU is available for use, and "False" if it is not available.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-BrokerRemotePCAccountNameAvailable -OU Test1
```

Checks whether the OU "Test1" is available.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-BrokerRemotePCAccountNameAvailable @("Test1","Test2","Test3")
```

Checks whether each of the specified names is available.

Update-BrokerImportedFTA

Sep 10, 2014

Imports or updates all of the file type associations for the specified worker.

Syntax

```
Update-BrokerImportedFTA -DesktopUids <Int32[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Imports or updates the file type associations from a specified worker machine.

File type association associates a file extension (such as ".txt") with an application (such as Notepad). In a Citrix environment file type associations on a user device can be configured so that when an user clicks on a document it launches the appropriate published application. This is known as "content redirection".

Imported file type associations are different from configured file type associations. Imported file type associations are lists of known file type associations for a given desktop group. Configured file type associations are those that are actually associated with published applications for the purposes of content redirection.

Initially the system is not aware of any extensions, and they must be imported by the Citrix administrator. To import or update file type associations from a worker machine, two criteria must be met:

o The worker machine must not be in use

o The worker machine must be in maintenance mode

For more information about putting a worker machine in maintenance mode, see the Set-BrokerPrivateDesktop and Set-BrokerSharedDesktop cmdlets.

Imported file type associations are grouped together based on the desktop group of the machine from which they were imported. All file types for a desktop group are deleted. There is no mechanism for deleting a subset imported file type associations for a specific desktop group.

If file type associations are imported more than once for a desktop group, for example, if this cmdlet is run twice for two workers belonging to the same desktop group, all existing imported file type associations for that desktop group are deleted and imported again.

Related topics

Get-BrokerImportedFTA

Remove-BrokerImportedFTA

Parameters

-DesktopUids<Int32[]>

Imports or updates the file type associations from the specified desktop. The desktop must belong to a desktop group of the Private or Shared desktop kind.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

Int32[] An array of Uids for desktops can be supplied as input.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $desktop = Get-BrokerSharedDesktop -MachineName "ACME\Worker1"
C:\PS> Set-BrokerSharedDesktop $desktop -InMaintenanceMode $true
C:\PS> Update-BrokerImportedFTA -DesktopUids $desktop.Uid
C:\PS> Set-BrokerSharedDesktop $desktop -InMaintenanceMode $false
```

Gets an object for the worker machine named "Worker1" in the "ACME" domain, and ensures no users can connect to it, before importing the file type associations from that desktop and re-enabling it.

Update-BrokerLocalLeaseCache

Sep 10, 2014

Flushes the local lease cache.

Syntax

```
Update-BrokerLocalLeaseCache [-Workers] [-Applications] [-Icons] [-Desktops] [-Leases] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Removes all local cached lease data and any state information stored in the registry.

Related topics

Remove-BrokerLease

Parameters

-Workers<SwitchParameter>

Removes all locally cached workers on the controller. The worker cache will be repopulated from the current site database contents after a short delay.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-Applications<SwitchParameter>

Removes all locally cached applications on the controller. The application cache will be repopulated from the current site database contents after a short delay.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-Icons<SwitchParameter>

Removes all locally cached icons on the controller. The icon cache will be repopulated from the current site database contents after a short delay.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-Desktops<SwitchParameter>

Removes all locally cached desktops on the controller. The desktop cache will be repopulated from the current site database contents after a short delay.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-Leases<SwitchParameter>

Removes all locally cached leases on the controller. The lease cache will be repopulated from the current site database contents after a short delay.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high level operation that this cmdlet call forms a part of. Desktop Studio and Desktop Director typically create High Level Operations. PowerShell scripts can also wrap a series of cmdlet calls in a High Level Operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None

Return Values

None

Notes

The local cache for lease and other data like worker, desktop, application and icon information is removed and will be repopulated from the current site database contents after a short delay.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Update-BrokerLocalLeaseCache
Flushes the local lease cache for all objects and deletes any state information stored in the registry.

---------- EXAMPLE 2 ----------

C:\PS> Update-BrokerLocalLeaseCache -Workers
Flushes the local lease cache for all workers and deletes any state information stored in the registry.

Update-BrokerNameCache

Sep 10, 2014

Performs administrative operations on the user and machine name cache.

Syntax

```
Update-BrokerNameCache [-Machines] [-Users] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Triggers an immediate asynchronous refresh of the name cache. This may be useful to ensure up-to-date name information is present in the cache after user and/or machine accounts are known to have changed and you need to see those changes immediately instead of waiting for the periodic automatic refresh.

The Broker Service maintains a cache of the names of users and machines in use by the site. By default, name information is obtained periodically from Active Directory and the cache refreshed automatically.

During normal usage, you should not need to perform administrative operations on the name cache.

For users/groups, the following name information is cached:

Windows name (DOMAIN\user)

User Principal Name or 'UPN' (user@upndomain)

Full Name or 'Common Name' (typically a user's full name)

For machines, the following name information is cached:

Windows name (DOMAIN\machine)

DNS name (machine.dnsdomain)

Related topics

Parameters

-Machines<SwitchParameter>

Triggers an asynchronous refresh of all cached machine name information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Users<SwitchParameter>

Triggers an asynchronous refresh of all cached user name information.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snapin will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

None

Notes

For some user accounts, for example, the built-in domain administrator, the UPN and/or Full Name values may not be available because they are not typically specified within Active Directory.

For group accounts, UPN and Full Name values are not available because they are not applicable or not specified within Active Directory.

The DNS name information for a machine is obtained from Active Directory and not from the DNS sub-system. If a machine has only recently been configured, the DNS information may not be available initially.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Update-BrokerNameCache -Machines
```

Triggers an immediate asynchronous refresh of all machine name information held within the name cache.

---------- EXAMPLE 2 ----------

```
C:\PS> Update-BrokerNameCache -Machines -Users
```

Triggers an immediate asynchronous refresh of all machine and user name information held within the name cache.

Citrix.Configuration.Admin.V2

Sep 10, 2014

Overview

Name	Description
ConfigConfigurationSnapin	The Configuration service PowerShell snap-in provides administrative
Config Filtering	Describes the common filtering options for XenDesktop cmdlets.

Cmdlets

Name	Description
Add-ConfigRegisteredServiceInstanceMetadata	Adds metadata on the given ServiceInstance.
Add-ConfigServiceGroupMetadata	Adds metadata on the given ServiceGroup.
Export-ConfigFeatureTable	Returns the current feature table.
Get-ConfigDBConnection	Gets the database string for the specified data store used by the Configuration Service.
Get-ConfigDBSchema	Gets a script that creates the Configuration Service database schema for the specified data store.
Get-ConfigDBVersionChangeScript	Gets a script that updates the Configuration Service database schema.
Get-ConfigEnabledFeature	Lists features of the site that are enabled.
Get-ConfigInstalledDBVersion	Gets a list of all available database schema versions for the Configuration Service.
Get-ConfigLicensingModel	Lists the supported licensing models.
Get-ConfigLocalData	Gets the service local data.
Get-ConfigProduct	Lists the site's supported product names and codes.
Get-ConfigProductEdition	Lists the supported product editions.

Name	Description
Get-ConfigProductFeature	Lists the supported features.
Get-ConfigProductVersion	Lists the supported product versions.
Get-ConfigRegisteredServiceInstance	Gets the service instances that are registered in the directory.
Get-ConfigService	Gets the service record entries for the Configuration Service.
Get-ConfigServiceAddedCapability	Gets any added capabilities for the Configuration Service on the controller.
Get-ConfigServiceGroup	Gets the service groups that match the parameters supplied.
Get-ConfigServiceInstance	Gets the service instance entries for the Configuration Service.
Get-ConfigServiceStatus	Gets the current status of the Configuration Service on the controller.
Get-ConfigSite	Gets the site.
Import-ConfigFeatureTable	Sets the feature table of the site.
Register-ConfigServiceInstance	Allows the registration of a service instance.
Remove-ConfigRegisteredServiceInstanceMetadata	Removes metadata from the given ServiceInstance.
Remove-ConfigServiceGroup	Removes service groups.
Remove-ConfigServiceGroupMetadata	Removes metadata from the given ServiceGroup.
Remove-ConfigServiceMetadata	Removes metadata from the given Service.
Remove-ConfigSiteMetadata	Removes metadata from the given Site.
Reset-ConfigServiceGroupMembership	Reloads the access permissions and configuration service locations for the Configuration Service.
Set-ConfigDBConnection	Configures a database connection for the Configuration Service.
Set-ConfigRegisteredServiceInstance	Updates a service instance.

Name	Description
Set-ConfigRegisteredServiceInstanceMetadata	Adds or updates metadata on the given ServiceInstance.
Set-ConfigServiceGroupMetadata	Adds or updates metadata on the given ServiceGroup.
Set-ConfigServiceMetadata	Adds or updates metadata on the given Service.
Set-ConfigSite	Changes the overall settings of the site.
Set-ConfigSiteMetadata	Adds or updates metadata on the Site.
Test-ConfigDBConnection	Tests a database connection for the Configuration Service.
Test-ConfigServiceInstanceAvailability	Tests whether the supplied service instances are responding to requests.
Unregister-ConfigRegisteredServiceInstance	Removes a service instance from the Configuration Service registry.

about_ConfigConfigurationSnapin

Sep 10, 2014

TOPIC

about_ConfigConfigurationSnapin

SHORT DESCRIPTION

The Configuration service PowerShell snap-in provides administrative functions for the Configuration service.

COMMAND PREFIX

All commands in this snap-in have 'Config' in their name.

LONG DESCRIPTION

The Configuration service PowerShell snap-in enables both local and remote administration of the Configuration service. It provides facilities to store details about other services that are used in the XenDesktop deployment.

All the services in the XenDesktop deployment use the Configuration service as a directory to locate other services with which they need to communicate. The directory publishes a list of all the services, the communication types they accept, and the facilities they offer.

The snap-in provides the following main entities:

Site Metadata

> Metadata for the entire XenDesktop deployment. This metadata is not used directly by any of the XenDesktop services, but can be used by third parties to store information for other purposes.

Registered Service Instances

> Service instance items that have been retrieved from the available services in the XenDesktop deployment and held in a directory in the Configuration service. Each physical service can host a collection of service instances to provide different facilities.

Service Groups

> A collection of service instances that are considered equivalent. Service instances that are registered in the same service group provide the same state and offer the same functionality.
>
> Only one service group of each type is supported. For example, there

must not be more than one service group with a ServiceType of 'Config'.

Site and Features

The configuration site is a top-level, logical representation of the XenDesktop site, from the perspective of the configuration services running within the site.

about_Config_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```

retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

```
A120901
B220000
...
```

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

Add-ConfigRegisteredServiceInstanceMetadata

Sep 10, 2014

Adds metadata on the given ServiceInstance.

Syntax

Add-ConfigRegisteredServiceInstanceMetadata [-ServiceInstanceUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ConfigRegisteredServiceInstanceMetadata [-ServiceInstanceUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ConfigRegisteredServiceInstanceMetadata [-InputObject] <ServiceInstance[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ConfigRegisteredServiceInstanceMetadata [-InputObject] <ServiceInstance[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given ServiceInstance objects. This cmdlet will not overwrite existing metadata on an object - use the Set-ConfigRegisteredServiceInstanceMetadata cmdlet instead.

Related topics

Set-ConfigRegisteredServiceInstanceMetadata

Remove-ConfigRegisteredServiceInstanceMetadata

Parameters

-ServiceInstanceUid<Guid>

Id of the ServiceInstance

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<ServiceInstance[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the ServiceInstance specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Configuration.Sdk.Metadata

Add-ConfigRegisteredServiceInstanceMetadata returns an array of objects containing the new definition of the metadata.

\n Property <string>

\n Specifies the name of the property.

\n Value <string>

\n Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DuplicateObject

One of the specified metadata already exists.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-ConfigRegisteredServiceInstanceMetadata -ServiceInstanceUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Property                       Value
        --------                      -----
        property                       value
```

Add metadata with a name of 'property' and a value of 'value' to the ServiceInstance with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Add-ConfigServiceGroupMetadata

Sep 10, 2014

Adds metadata on the given ServiceGroup.

Syntax

Add-ConfigServiceGroupMetadata [-ServiceGroupUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ConfigServiceGroupMetadata [-ServiceGroupUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ConfigServiceGroupMetadata [-InputObject] <ServiceGroup[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ConfigServiceGroupMetadata [-InputObject] <ServiceGroup[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given ServiceGroup objects. This cmdlet will not overwrite existing metadata on an object - use the Set-ConfigServiceGroupMetadata cmdlet instead.

Related topics

Set-ConfigServiceGroupMetadata

Remove-ConfigServiceGroupMetadata

Parameters

-ServiceGroupUid<Guid>

Id of the ServiceGroup

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<ServiceGroup[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the ServiceGroup specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Configuration.Sdk.Metadata

Add-ConfigServiceGroupMetadata returns an array of objects containing the new definition of the metadata.

\n Property <string>

\n Specifies the name of the property.

\n Value <string>

\n Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DuplicateObject

One of the specified metadata already exists.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Add-ConfigServiceGroupMetadata -ServiceGroupUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

    Property                  Value
    --------                  -----
    property                  value
```


Add metadata with a name of 'property' and a value of 'value' to the ServiceGroup with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Export-ConfigFeatureTable

Sep 10, 2014

Returns the current feature table.

Syntax

Export-ConfigFeatureTable [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Related topics

Set-ConfigSite

Import-ConfigFeatureTable

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Export-ConfigFeatureTable
<?xml version="1.0" encoding="utf-8">
<Products xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="FeatureTable.xsd">
 <Product Code="XDT" Name="XenDesktop">
  <Editions>
   <Edition>PLT</Edition>
   <Edition>ENT</Edition>
   <Edition>APP</Edition>
   <Edition>STD</Edition>
  </Editions>
  <DefaultEdition>PLT</DefaultEdition>
  <VersionToBurninDates>
   <VersionToBurninDate Version="7.0" BurninDate="2013.0522" />
  </VersionToBurninDates>
  <LicensingModels>
   <LicensingModel>Concurrent</LicensingModel>
   <LicensingModel>UserDevice</LicensingModel>
  </LicensingModels>
  <DefaultLicensingModel>UserDevice</DefaultLicensingModel>
  <Features>
   <Feature Name="CustomRole">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="APP" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="ConfigurationLogging">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="APP" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="SingleUserMode">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
```

```
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="MultiSessionDesktops">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="APP" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="SingleSessionDesktops">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="STD" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="MultiSessionApplications">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="APP" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="SingleSessionApplications">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="APP" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="HistoricalMonitorData">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="CloudHostedMachines">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="HdxInsightIntegration">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="RemotePC">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
  </Features>
</Product>
<Product Code="MPS" Name="XenApp">
  <Editions>
   <Edition>PLT</Edition>
   <Edition>ENT</Edition>
  </Editions>
  <DefaultEdition>PLT</DefaultEdition>
  <VersionToBurninDates>
   <VersionToBurninDate Version="7.0" BurninDate="2013.0522" />
  </VersionToBurninDates>
  <LicensingModels>
   <LicensingModel>Concurrent</LicensingModel>
  </LicensingModels>
  <DefaultLicensingModel>Concurrent</DefaultLicensingModel>
  <Features>
   <Feature Name="CustomRole">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="ConfigurationLogging">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="SingleUserMode">
   </Feature>
   <Feature Name="MultiSessionDesktops">
    <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
    <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
   </Feature>
   <Feature Name="SingleSessionDesktops">
   </Feature>
   <Feature Name="MultiSessionApplications">
```

```
      <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
      <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
    </Feature>
    <Feature Name="SingleSessionApplications">
      <BurninDate ForProductEdition="PLT" MustBe="AtLeast">2013.0522</BurninDate>
      <BurninDate ForProductEdition="ENT" MustBe="AtLeast">2013.0522</BurninDate>
    </Feature>
    <Feature Name="HistoricalMonitorData">
    </Feature>
    <Feature Name="CloudHostedMachines">
    </Feature>
    <Feature Name="HdxInsightIntegration">
    </Feature>
    <Feature Name="RemotePC">
    </Feature>
   </Features>
  </Product>
</Products>
```

Returns the current feature table.

Get-ConfigDBConnection

Sep 10, 2014

Gets the database string for the specified data store used by the Configuration Service.

Syntax

```
Get-ConfigDBConnection [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the database connection string for the specified data store.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

Related topics

Get-ConfigServiceStatus

Set-ConfigDBConnection

Test-ConfigDBConnection

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

system.string

The database connection string configured for the Configuration Service.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the Configuration Service has not been specified.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-ConfigDBConnection

Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True
```

Get the database connection string for the Configuration Service.

Get-ConfigDBSchema

Sep 10, 2014

Gets a script that creates the Configuration Service database schema for the specified data store.

Syntax

Get-ConfigDBSchema [-DatabaseName <String>] [-ServiceGroupName <String>] [-ScriptType <ScriptTypes>] [-LocalDatabase] [-Sid <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets SQL scripts that can be used to create a new Configuration Service database schema, add a new Configuration Service to an existing site, remove a Configuration Service from a site, or create a database server logon for a Configuration Service. If no Sid parameter is provided, the scripts obtained relate to the currently selected Configuration Service instance, otherwise the scripts relate to Configuration Service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied. The current service instance is that on the local machine, or that explicitly specified by the last usage of the -AdminAddress parameter to a Configuration SDK cmdlet. The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured. The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SMDCMD mode'. The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to Configuration Service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to Configuration Service roles

If ScriptType is Evict, the returned script contains:

o Removal of Configuration Service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database. You do not need to configure a database before using this command.

Related topics

Parameters

-DatabaseName<String>

Specifies the name of the database for which the schema will be generated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the Configuration services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<ScriptTypes>

Specifies the type of database script returned. Available script types are:

Database

Returns a full database script that can be used to create a database schema for the Configuration Service in a database instance that does not already contain a schema for this service. The DatabaseName and ServiceGroupName parameters must be specified to create a script of this type.

Instance

Returns a permissions script that can be used to add further Configuration services to an existing database instance that already contains the full Configuration service schema, associating the services to the Service Group. The Sid parameter can optionally be specified to create a script of this type.

Login

Returns a database logon script that can be used to add the required logon accounts to an existing database instance that contains the Configuration Service schema. This is used primarily when creating a mirrored database environment. The DatabaseName parameter must be specified to create a script of this type.

Evict

Returns a script that can be used to remove the specified Configuration Service from the database entirely. The DatabaseName and Sid parameters must be specified to create a script of this type.

Required?	false
Default Value	Database
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for Configuration services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Sid<String>

Specifies the SID of the controller on which the Configuration Service instance to remove from the database is running.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.string

A string containing the required SQL script for application to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigDBSchema -DatabaseName MyDB -ServiceGroupName  MyServiceGroup > c:\ConfigSchema.sql
```

Get the full database schema for site data store of the Configuration Service and copy it to a file called 'c:\ConfigSchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a Configuration Service site schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigDBSchema -DatabaseName MyDB -scriptType Login > c:\ConfigurationLogins.sql
```

Get the logon scripts for the Configuration Service.

Get-ConfigDBVersionChangeScript

Sep 10, 2014

Gets a script that updates the Configuration Service database schema.

Syntax

Get-ConfigDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns a database script that can be used to upgrade or downgrade the site or secondary schema for the Configuration Service from the current schema version to a different version.

Related topics

Get-ConfigInstalledDBVersion

Parameters

-DatabaseName<String>

Specifies the name of the database instance to which the update applies.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

Specifies the version of the database you want to update to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

A PSObject containing the required SQL script for application to a database.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any Configuration services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-ConfigServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Configuration Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS> $update = Get-ConfigDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-ConfigEnabledFeature

Sep 10, 2014

Lists features of the site that are enabled.

Syntax

```
Get-ConfigEnabledFeature [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Related topics

Set-ConfigSite

Import-ConfigFeatureTable

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-ConfigEnabledFeature
```

Retrieves the list of enabled features for the site's current configuration.

Get-ConfigInstalledDBVersion

Sep 10, 2014

Gets a list of all available database schema versions for the Configuration Service.

Syntax

```
Get-ConfigInstalledDBVersion [-Upgrade] [-Downgrade] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the current version of the Configuration Service database schema, if no flags are set, otherwise returns versions for which upgrade or downgrade scripts are available and have been stored in the database.

Related topics

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Version

The Get-ConfigInstalledDbVersion command returns objects containing the new definition of the Configuration Service database schema version.

Major <Integer>

Minor <Integer>

Build <Integer>

Revision <Integer>

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Configuration Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigInstalledDBVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      6      0      0
```

Get the currently installed version of the Configuration Service database schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigInstalledDBVersion -Upgrade

Major  Minor  Build  Revision
-----  -----  -----  --------
6      0      0      0
```

Get the versions of the Configuration Service database schema for which upgrade scripts are supplied.

Get-ConfigLicensingModel

Sep 10, 2014

Lists the supported licensing models.

Syntax

```
Get-ConfigLicensingModel -ProductCode <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Related topics

Get-ConfigProduct

Get-ConfigSite

Set-ConfigSite

Import-ConfigFeatureTable

Parameters

-ProductCode<String>

The product code

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

The list of supported licensing models for the specified product code.

Notes

The Get-ConfigProduct cmdlet lists the available product codes.

The site object returned by the Get-ConfigSite cmdlet contains the currently configured product code.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-ConfigLicensingModel -ProductCode "XDS"
```

Retrieves the list of supported licensing models for product code "XDS".

Get-ConfigLocalData

Sep 10, 2014

Gets the service local data.

Syntax

```
Get-ConfigLocalData [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Get-ConfigLocalData returns service-and-controller-specific local data. This information is not site-wide, but rather controller-specific. The Configuration Service currently stores the controller product version as local data. The overall site version used by Studio is an aggregate of the product versions from each controller.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

This cmdlet does not accept pipeline input

Return Values

Citrix.Configuration.DataModel.LocalData

Contains the ControllerProductVersion field

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-ConfigLocalData

ControllerProductVersion
-----------
7.1
```

Gets the service local data.

Get-ConfigProduct

Sep 10, 2014

Lists the site's supported product names and codes.

Syntax

```
Get-ConfigProduct [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Related topics

Get-ConfigSite

Set-ConfigSite

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

PSObject

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-ConfigProduct
```

Lists the supported products by name and code.

Get-ConfigProductEdition

Sep 10, 2014

Lists the supported product editions.

Syntax

```
Get-ConfigProductEdition [-ProductCode] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Related topics

Get-ConfigProduct

Get-ConfigSite

Set-ConfigSite

Import-ConfigFeatureTable

Parameters

-ProductCode<String>

The product code

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

The list of supported licensing models for the specified product code.

Notes

The Get-ConfigProduct cmdlet lists the available product codes.

The site object returned by Get-ConfigSite cmdlet contains the currently configured product code.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-ConfigProductEdition -ProductCode "XDS"
```

Retrieves the list of supported editions for XenDesktop.

Get-ConfigProductFeature

Sep 10, 2014

Lists the supported features.

Syntax

```
Get-ConfigProductFeature [-ProductCode] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Lists the supported features. Use the Get-ConfigEnabledFeature command to determine which features are currently enabled.

Related topics

Get-ConfigProduct

Get-ConfigSite

Set-ConfigSite

Import-ConfigFeatureTable

Parameters

-ProductCode<String>

The product code

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

The list of supported licensing models for the specified product code.

Notes

The Get-ConfigProduct cmdlet lists the available product codes.

The site object returned by Get-ConfigSite cmdlet contains the currently configured product code.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-ConfigProductFeature -ProductCode "XDS"
```

Retrieves the list of supported features for XenDesktop.

Get-ConfigProductVersion

Sep 10, 2014

Lists the supported product versions.

Syntax

```
Get-ConfigProductVersion [-ProductCode] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Related topics

Get-ConfigProduct

Get-ConfigSite

Set-ConfigSite

Import-ConfigFeatureTable

Parameters

-ProductCode<String>

The product code

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

The list of supported licensing models for the specified product code.

Notes

The Get-ConfigProduct cmdlet lists the available product codes.

The site object returned by Get-ConfigSite cmdlet contains the currently configured product code.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-ConfigProductVersion -ProductCode "XDS"
```

Retrieves the list of supported versions for XenDesktop.

Get-ConfigRegisteredServiceInstance

Sep 10, 2014

Gets the service instances that are registered in the directory.

Syntax

```
Get-ConfigRegisteredServiceInstance [-ServiceInstanceUid <Guid>] [-ServiceGroupUid <Guid>] [-ServiceGroupName <String>] [-ServiceType <String>] [-Address <String>] [-Binding <String>] [-Version <Int32>] [-ServiceAccountSid <String>] [-InterfaceType <String>] [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this cmdlet to retrieve the service instances currently registered with the Configuration Service that match the parameters supplied. If no parameters are supplied, all the service instances are returned.

Related topics

Register-ConfigServiceInstance

Unregister-ConfigRegisteredServiceInstance

Set-ConfigRegisteredServiceInstance

Parameters

-ServiceInstanceUid<Guid>

The unique identifier for the service instance.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupUid<Guid>

The unique identifier for the service group to which the service instance belongs.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

The name for the service group to which the service instance belongs.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceType<String>

The service type for the service instance.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Address<String>

The connection address for the service instance.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Binding<String>

The binding for the service instance.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Version<Int32>

The service instance version.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceAccountSid<String>

The AD account SID for the computer account that the computer hosting the service instance is running as.

Required?	false
Default Value	
Accept Pipeline Input?	false

-InterfaceType<String>

The interface type for the service instance.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

See about_Config_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

See about_Config_Filtering for details.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

See about_Config_Filtering for details.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

See about_Config_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Filter<String>

See about_Config_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Configuration.Sdk.ServiceInstance

This represents a service instance and has the following parameters;

ServiceGroupUid <Guid>

The unique identifier for the service group to which the service instance belongs.

ServiceGroupName <string>

The name of the service group to which the service instance belongs.

ServiceInstanceUid <Guid>

The unique identifier for the service instance.

ServiceType <string>

The type of the service group.

Address <string>

The contact address for the service instance.

Binding <string>

The binding to use for connections to the service instance.

Version <int>

The version of the service instance.

ServiceAccount <string>

The AD computer account for the computer that is providing the service instance.

ServiceAccountSid <string>

The AD computer account SID for the computer that is providing the service instance.

InterfaceType <string>

The interface type for the service instance.

Metadata <Citrix.Configuration.Sdk.Metadata[]>

The metadata for the service instance.

Notes

In the case of failure, the following errors can result.

Error Codes ---------- PartialData Only a subset of the available data was returned. CouldNotQuueryDatabase The query required to get the database was not defined. CommunicationError An error occurred while communicating with the service. DatabaseNotConfigured The operation could not be completed because the database for the service is not configured. InvalidFilter A filtering expression was supplied that could not be interpreted for this cmdlet. ExceptionThrown An unexpected error occurred. To locate more details see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\>Get-ConfigRegisteredServiceInstance

Address         : http://MyServer.com:80/Citrix/MyContract/v1
Binding         : wcf_HTTP_kerb
```



```
InterfaceType     : SDK
Metadata          : {}
MetadataMap       : {}
ServiceAccount    : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-1155438255-2213498043-2452000591-1104
ServiceGroupName  : MyService
ServiceGroupUid   : 2b990d5a-bba9-413b-aa08-e104e67f89bc
ServiceInstanceUid : 8dc38b5a-3fbb-457c-b326-6c41c94c18d5
ServiceType       : MySnapIn
Version           : 1

Address           : http://MyServer.com:80/Citrix/MyContract/PeerAPI/v1
Binding           : wcf_HTTP_kerb
InterfaceType     : Peer
Metadata          : {}
MetadataMap       : {}
ServiceAccount    : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-1155438255-2213498043-2452000591-1104
ServiceGroupName  : MyService
ServiceGroupUid   : 2b990d5a-bba9-413b-aa08-e104e67f89bc
ServiceInstanceUid : 8f822ed6-42f3-4a26-911a-a4a6a87c0ef2
ServiceType       : MySnapIn
Version           : 1

Address           : http://MyServer.com:80/Citrix/MyContract/MyServiceEnvTestAPI/v1
Binding           : wcf_HTTP_kerb
InterfaceType     : EnvironmentTest
Metadata          : {}
MetadataMap       : {}
ServiceAccount    : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-1155438255-2213498043-2452000591-1104
ServiceGroupName  : MyService
ServiceGroupUid   : 2b990d5a-bba9-413b-aa08-e104e67f89bc
ServiceInstanceUid : d2d40d9b-2a5d-4c5a-b9ca-a7f73cffe4f2
ServiceType       : MySnapIn
Version           : 1

Address           : http://MyServer.com:80/Citrix/MyContract/MyServiceAPI/v1
Binding           : wcf_HTTP_kerb
InterfaceType     : InterService
Metadata          : {}
MetadataMap       : {}
ServiceAccount    : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-1155438255-2213498043-2452000591-1104
ServiceGroupName  : MyService
ServiceGroupUid   : 2b990d5a-bba9-413b-aa08-e104e67f89bc
ServiceInstanceUid : 5d428970-2ba1-4336-b8d0-f3aa961b8983
ServiceType       : MySnapIn
```

```
Version          : 1
```
Return all the service instances that are registered in the Configuration Service.

-------------------------- EXAMPLE 2 --------------------------

```
C:\>Get-ConfigRegisteredServiceInstance -InterfaceType "SDK"

Address          : http://MyServer.com:80/Citrix/MyContract/v1
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         : {}
MetadataMap      : {}
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-1155438255-2213498043-2452000591-1104
ServiceGroupName  : MyService
ServiceGroupUid   : 2b990d5a-bba9-413b-aa08-e104e67f89bc
ServiceInstanceUid : 8dc38b5a-3fbb-457c-b326-6c41c94c18d5
ServiceType      : MySnapIn
Version          : 1
```
Return all the service instances that are registered in the Configuration Service and are of type 'SDK'.

Get-ConfigService

Sep 10, 2014

Gets the service record entries for the Configuration Service.

Syntax

Get-ConfigService [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns instances of the Configuration Service that the service publishes. The service records contain account security identifier information that can be used to remove each service from the database.

A database connection for the service is required to use this command.

Related topics

Parameters

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Config_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Config_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Configuration.Sdk.Service

The Get-ConfigServiceInstance command returns an object containing the following properties.

Uid <Integer>

Specifies the unique identifier for the service in the group. The unique identifier is an index number.

ServiceHostId <Guid>

Specifies the unique identifier for the service instance.

DNSName <String>

Specifies the domain name of the host on which the service runs.

MachineName <String>

Specifies the short name of the host on which the service runs.

CurrentState <Citrix.Fma.Sdk.ServiceCore.ServiceState>

Specifies whether the service is running, started but inactive, stopped, or failed.

LastStartTime <DateTime>

Specifies the date and time at which the service was last restarted.

LastActivityTime <DateTime>

Specifies the date and time at which the service was last stopped or restarted.

OSType

Specifies the operating system installed on the host on which the service runs.

OSVersion

Specifies the version of the operating system installed on the host on which the service runs.

ServiceVersion

Specifies the version number of the service instance. The version number is a string that reflects the full build version of the service.

DatabaseUserName <string>

Specifies for the service instance the Active Directory account name with permissions to access the database. This will be either the machine account or, if the database is running on a controller, the NetworkService account.

Sid <string>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

ActiveSiteServices <string[]>

Specifies the names of active site services currently running in the service. Site services are components that perform long-running background processing in some services. This field is empty for services that do not contain site services.

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigService

Uid             : 1
ServiceHostId   : aef6f464-f1ee-4042-a523-66982e0cecd0
DNSName         : MyServer.company.com
MachineName     : MYSERVER
CurrentState    : On
LastStartTime   : 04/04/2011 15:25:38
LastActivityTime : 04/04/2011 15:33:39
OSType          : Win32NT
OSVersion       : 6.1.7600.0
ServiceVersion  : 5.1.0.0
DatabaseUserName : NT AUTHORITY\NETWORK SERVICE
SID             : S-1-5-21-2316621082-1546847349-2782505528-1165
ActiveSiteServices : {MySiteService1, MySiteService2...}
```

Get all the instances of the Configuration Service running in the current service group.

Get-ConfigServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the Configuration Service on the controller.

Syntax

```
Get-ConfigServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the Configuration Service on the controller to be detected.

You do not need to configure a database connection before using this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigServiceAddedCapability
```

Get the added capabilities of the Configuration Service.

Get-ConfigServiceGroup

Sep 10, 2014

Gets the service groups that match the parameters supplied.

Syntax

```
Get-ConfigServiceGroup [-ServiceGroupUid <Guid>] [-ServiceGroupName <String>] [-ServiceType <String>] [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this cmdlet to retrieve existing service groups that match the parameters supplied. If no parameters are supplied, all the service groups are returned.

Related topics

Parameters

-ServiceGroupUid<Guid>

The unique identifier for the service group.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceType<String>

The service type for the service group.

Required?	false

Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

See about_Config_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

See about_Config_Filtering for details.

Required?	false

Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

See about_Config_Filtering for details.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

See about_Config_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Filter<String>

See about_Config_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Configuration.Sdk.ServiceGroup

This represents a service instance and has the following parameters;

ServiceGroupUid <Guid>

The unique identifier for the service group.

ServiceGroupName <string>

The name of the service group.

ServiceType <string>

The type of the service group.

Metadata <Citrix.Configuration.Sdk.Metadata[]>

The metadata for the service group.

Notes

In the case of failure, the following errors can result.

Error Codes ----------

DatabaseNotConfigured The operation could not be completed because the database for the service is not configured. PartialData Only a subset of the available data was returned. CouldNotQuueryDatabase The Query required to get the database was not defined. CommunicationError An error occurred while communicating with the service. InvalidFilter A filtering expression was supplied that could not be interpreted for this cmdlet. ExceptionThrown An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

C:\>Get-ConfigServiceGroup
Return all the service groups that are registered in the Configuration Service.

---------- EXAMPLE 2 ----------

C:\>Get-ConfigRegisteredServiceInstance -ServiceType "config"
Return all the service groups that are registered in the Configuration Service and are of type 'config' (i.e. the service groups for the Configuration Service).

Get-ConfigServiceInstance

Sep 10, 2014

Gets the service instance entries for the Configuration Service.

Syntax

```
Get-ConfigServiceInstance [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns service interfaces published by the instance of the Configuration Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Configuration.Sdk.ServiceInstance

The Get-ConfigServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a

central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

Specifies the service instance type. For this service, the service instance type is always Config.

Address

Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

SDK - for PowerShell operations

InterService - for operations between different services

Peer - for communications between services of the same type

Metadata <Citrix.Configuration.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigServiceInstance

Address          : http://MyServer.com:80/Citrix/ConfigurationService
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         :
MetadataMap      :
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName  : MyServiceGroup
ServiceGroupUid   : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType      : Config
Version          : 1

Address          : http://MyServer.com:80/Citrix/ConfigurationService/IServiceApi
Binding          : wcf_HTTP_kerb
InterfaceType    : InterService
Metadata         :
MetadataMap      :
```



```
ServiceAccount     : ENG\MyAccount
ServiceAccountSid  : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName   : MyServiceGroup
ServiceGroupUid    : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType        : Config
Version            : 1
```

Get all instances of the Configuration Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-ConfigServiceStatus

Sep 10, 2014

Gets the current status of the Configuration Service on the controller.

Syntax

```
Get-ConfigServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the Configuration Service on the controller to be monitored. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured.

Related topics

Set-ConfigDBConnection

Test-ConfigDBConnection

Get-ConfigDBConnection

Get-ConfigDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-ConfigServiceStatus command returns an object containing the status of the Configuration Service together with extra diagnostics information.

DBUnconfigured

The Configuration Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the Configuration Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Configuration Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Configuration Service currently in use is incompatible with the version of the Configuration Service schema on the database. Upgrade the Configuration Service to a more recent version.

DBOlderVersionThanService

The version of the Configuration Service schema on the database is incompatible with the version of the Configuration Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Configuration Service is running and is connected to a database containing a valid schema.

Failed

The Configuration Service has failed.

Unknown

(0) The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigServiceStatus

DBUnconfigured
```

Get the current status of the Configuration Service.

Get-ConfigSite

Sep 10, 2014

Gets the site.

Syntax

```
Get-ConfigSite [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Get-ConfigSite cmdlet gets the site.

A XenDesktop installation has only a single site instance.

Related topics

Set-ConfigSite

Import-ConfigFeatureTable

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Get-ConfigSite returns the site instance.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-ConfigSite
```

Gets the site.

Import-ConfigFeatureTable

Sep 10, 2014

Sets the feature table of the site.

Syntax

```
Import-ConfigFeatureTable [-Path] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Import-ConfigFeatureTable -Content <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Related topics

Export-ConfigFeatureTable

Get-ConfigSite

Set-ConfigSite

Get-ConfigProduct

Get-ConfigProductEdition

Get-ConfigProductFeature

Get-ConfigProductVersion

Get-ConfigLicensingModel

Parameters

-Path<String>

The path to the file containing the feature table

Required?	true
Default Value	
Accept Pipeline Input?	false

-Content<String>

Set the site's feature table.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Import-ConfigFeatureTable $xml
```

Specifies the use of a Platinum edition license. A suitable license must be available on the site's license server.

Register-ConfigServiceInstance

Sep 10, 2014

Allows the registration of a service instance.

Syntax

Register-ConfigServiceInstance -ServiceGroupUid <Guid> -ServiceGroupName <String> -ServiceType <String> -Address <String> -Binding <String> -Version <Int32> -ServiceAccountSid <String> -InterfaceType <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Register-ConfigServiceInstance -ServiceGroupUid <Guid> -ServiceGroupName <String> -ServiceType <String> -Address <String> -Binding <String> -Version <Int32> -ServiceAccount <String> -InterfaceType <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Register-ConfigServiceInstance -ServiceInstance <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Use this cmdlet to register service instance items in the Configuration Service. Service instances can be registered either by retrieving the data directly from other services or by manually entering the details into this command.

If the service group specified by the service instance already exists, the service is added to the service group, otherwise a new service group is created to hold the service instance.

Related topics

Unregister-ConfigRegisteredServiceInstance

Add-ConfigRegisteredServiceInstanceMetadata

Set-ConfigRegisteredServiceInstanceMetadata

Remove-ConfigRegisteredServiceInstanceMetadata

Add-ConfigServiceGroupMetadata

Set-ConfigServiceGroupMetadata

Remove-ConfigServiceGroupMetadata

Parameters

-ServiceGroupUid<Guid>

The Service Group Unique Identifier

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ServiceGroupName<String>

The name of the service group

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ServiceType<String>

The type of the service group

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Address<String>

The address that is used to access the service instance.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Binding<String>

The binding type that must be used to access the service instance.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Version<Int32>

The version of the service instance.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ServiceAccountSid<String>

The AD computer account Sid for the computer on which the service instance is hosted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-InterfaceType<String>

The type of interface that the service provides (i.e. SDK, InterService, Peer).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ServiceAccount<String>

The AD computer account name (domain qualified) for the computer on which the service instance is hosted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ServiceInstance<ServiceInstance[]>

The service instances to register.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the logging id of the high-level operation that this cmdlet is part of.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can be provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.Configuration.Sdk.ServiceInstance An object with the following parameters can be used to register a service instance. Address, ServiceGroupUid, ServiceGroupName, ServiceType, Binding, Version, InterfaceType.

Return Values

Citrix.Configuration.Sdk.ServiceInstance

This represents a service instance and has the following parameters;

ServiceGroupUid <Guid>

The unique identifier for the service group to which the service instance belongs.

ServiceGroupName <string>

The name of the service group to which the service instance belongs.

ServiceInstanceUid <Guid>

The unique identifier for the service instance.

ServiceType <string>

The type of the service group.

Address <string>

The contact address for the service instance.

Binding <string>

The binding to use for connections to the service instance.

Version <int>

The version of the service instance.

ServiceAccount <string>

The AD computer account for the computer that is providing the service instance.

ServiceAccountSid <string>

The AD computer account SID for the computer that is providing the service instance.

InterfaceType <string>

The interface type for the service instance.

Metadata <Citrix.Configuration.Sdk.Metadata[]>

The metadata for the service instance.

Notes

In the case of failure, the following errors can result.

Error Codes ---------- ActiveDirectoryAccountResolutionFailed The account name provided could not be found in Active Directory. ServiceGroupWithSameUidExistsForDifferentServiceGroupNameOrSameUidExistsForDifferentServiceGroupNameOrServiceType The service group name or service type do not match the service group found with the specified uid. TypeAlreadyExists A different service group with the same type is registered already in the Configuration Service. DatabaseError An error occurred in the service while attempting a database operation. DatabaseNotConfigured The operation could not be completed because the database for the service is not configured. DataStoreException An error occurred in the service while attempting a database operation - communication with the database failed for various reasons. CommunicationError An error occurred while communicating with the service. ExceptionThrown An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

C:\PS>Get-ConfigServiceInstance | Register-ConfigServiceInstance
Gets the service instances for the Configuration Service and registers them.

Remove-ConfigRegisteredServiceInstanceMetadata

Sep 10, 2014

Removes metadata from the given ServiceInstance.

Syntax

```
Remove-ConfigRegisteredServiceInstanceMetadata [-ServiceInstanceUid] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ConfigRegisteredServiceInstanceMetadata [-ServiceInstanceUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ConfigRegisteredServiceInstanceMetadata [-InputObject] <ServiceInstance[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ConfigRegisteredServiceInstanceMetadata [-InputObject] <ServiceInstance[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given ServiceInstance.

Related topics

Add-ConfigRegisteredServiceInstanceMetadata

Set-ConfigRegisteredServiceInstanceMetadata

Parameters

-ServiceInstanceUid<Guid>

Id of the ServiceInstance

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<ServiceInstance[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigServiceInstance | Remove-ConfigRegisteredServiceInstanceMetadata
```

Remove all metadata from all ServiceInstance objects.

Remove-ConfigServiceGroup

Sep 10, 2014

Removes service groups.

Syntax

```
Remove-ConfigServiceGroup [-ServiceGroupUid] <Guid> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this cmdlet to remove a service group and all the service instances that it contains.

Related topics

Register-ConfigServiceInstance

Add-ConfigServiceGroupMetadata

Set-ConfigServiceGroupMetadata

Remove-ConfigServiceGroupMetadata

Parameters

-ServiceGroupUid<Guid>

The unique identifier for the service group.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the logging id of the high-level operation this cmdlet invocation is part of.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

In the case of failure, the following errors can result.

Error Codes ---------- ServiceGroupObjectNotFound The service group specified could not be located. DatabaseError An error occurred in the service while attempting a database operation. DatabaseNotConfigured The operation could not be completed because the database for the service is not configured. DataStoreException An error occurred in the service while attempting a database operation - communication with the database failed for various reasons. CommunicationError An error occurred while communicating with the service. ExceptionThrown An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

C:\PS>Remove-ConfigServiceGroup -ServiceGroupUid 31951f6f-7703-4abb-938a-2861d76ecfea
Removes the service group (and all contained service instances) for the service group with a unique identifier of '31951f6f-7703-4abb-938a-2861d76ecfea'.

---------- EXAMPLE 2 ----------

C:\PS> Get-configServiceGroup | remove-ConfigServiceGroup
Removes all the service groups (and all contained service instances) for the XenDesktop deployment.

Remove-ConfigServiceGroupMetadata

Sep 10, 2014

Removes metadata from the given ServiceGroup.

Syntax

```
Remove-ConfigServiceGroupMetadata [-ServiceGroupUid] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ConfigServiceGroupMetadata [-ServiceGroupUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ConfigServiceGroupMetadata [-InputObject] <ServiceGroup[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ConfigServiceGroupMetadata [-InputObject] <ServiceGroup[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given ServiceGroup.

Related topics

Add-ConfigServiceGroupMetadata

Set-ConfigServiceGroupMetadata

Parameters

-ServiceGroupUid<Guid>

Id of the ServiceGroup

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<ServiceGroup[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigServiceGroup | % { Remove-ConfigServiceGroupMetadata -Map $_.MetadataMap }
```

Remove all metadata from all ServiceGroup objects.

Remove-ConfigServiceMetadata

Sep 10, 2014

Removes metadata from the given Service.

Syntax

```
Remove-ConfigServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ConfigServiceMetadata [-ServiceHostId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ConfigServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ConfigServiceMetadata [-InputObject] <Service[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Service.

Related topics

Set-ConfigServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigService | % { Remove-ConfigServiceMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Service objects.

Remove-ConfigSiteMetadata

Sep 10, 2014

Removes metadata from the given Site.

Syntax

```
Remove-ConfigSiteMetadata -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

```
Remove-ConfigSiteMetadata -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Site.

Related topics

Set-ConfigSiteMetadata

Parameters

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for

various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-ConfigSite | % { Remove-ConfigSiteMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Site objects.

Reset-ConfigServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the Configuration Service.

Syntax

```
Reset-ConfigServiceGroupMembership [-ConfigServiceInstance] <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Enables you to reload Configuration Service access permissions and configuration service locations. The Reset-ConfigServiceGroupMembership command must be run on at least one instance of the service type (Config) after installation and registration with the configuration service. Without this operation, the Configuration services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-ConfigServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Parameters

-ConfigServiceInstance<ServiceInstance[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.Configuration.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-ConfigServiceGroupMembership command.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-ConfigServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-ConfigServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Set-ConfigDBConnection

Sep 10, 2014

Configures a database connection for the Configuration Service.

Syntax

```
Set-ConfigDBConnection [-DBConnection] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Configures a connection to a database in which the Configuration Service can store its state. The service will attempt to connect and start using the database immediately after the connection is configured. The database connection string is updated to the specified value regardless of whether it is valid or not. Specifying an invalid connection string prevents a service from functioning until the error is corrected.

After a connection is configured, you cannot alter it without first clearing it (by setting the connection to $null).

You do not need to configure a database connection to use this command.

Related topics

Get-ConfigServiceStatus

Get-ConfigDBConnection

Test-ConfigDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the Configuration Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-ConfigDBConnection command returns an object containing the status of the Configuration Service together with extra diagnostics information.

DBUnconfigured

The Configuration Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the Configuration Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Configuration Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Configuration Service currently in use is incompatible with the version of the Configuration Service schema on the database. Upgrade the Configuration Service to a more recent version.

DBOlderVersionThanService

The version of the Configuration Service schema on the database is incompatible with the version of the Configuration Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Configuration Service is running and is connected to a database containing a valid schema.

Failed

The Configuration Service has failed.

Unknown

The status of the Configuration Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-ConfigDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Configures a database connection string for the Configuration Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Set-ConfigDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Configures an invalid database connection string for the Configuration Service.

Set-ConfigRegisteredServiceInstance

Sep 10, 2014

Updates a service instance.

Syntax

```
Set-ConfigRegisteredServiceInstance -ServiceInstanceUid <Guid> -Address <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Use this cmdlet to change the address property of an existing service instance that is registered in the Configuration Service.

Related topics

Get-ConfigRegisteredServiceInstance

Register-ConfigServiceInstance

Unregister-ConfigRegisteredServiceInstance

Parameters

-ServiceInstanceUid<Guid>

The unique identifier for the service instance to be updated.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Address<String>

The new address for the service instance.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Defines whether or not the command returns a result showing the new state of the updated service instance.

Required?	false
Default Value	true
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the logging id of the high-level operation this cmdlet invocation is part of.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Configuration.Sdk.ServiceInstance

This represents a service instance and has the following parameters:

ServiceGroupUid <Guid>

The unique identifier for the service group to which the service instance belongs.

ServiceGroupName <string>

The name of the service group to which the service instance belongs.

ServiceInstanceUid <Guid>

The unique identifier for the service instance.

ServiceType <string>

The type of the service group.

Address <string>

The contact address for the service instance.

Binding <string>

The binding to use for connections to the service instance.

Version <int>

The version of the service instance.

ServiceAccount <string>

The AD computer account for the computer that is providing the service instance.

ServiceAccountSid <string>

The AD computer account SID for the computer that is providing the service instance.

InterfaceType <string>

The interface type for the service instance.

Metadata <Citrix.Configuration.Sdk.Metadata[]>

The metadata for the service instance.

Notes

In the case of failure, the following errors can result.

Error Codes ---------- ObjectToUpdateDoesNotExist The service instance specified could not be located. DatabaseError An error occurred in the service while attempting a database operation. DatabaseNotConfigured The operation could not be completed because the database for the service is not configured. DataStoreException An error occurred in the service while attempting a database operation - communication with the database failed for various reasons. CommunicationError An error occurred while communicating with the service. ExceptionThrown An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Set-ConfigResgisteredService -ServiceInstanceUid "9805f39d-99eb-44f0-8f63-9d8e3f1228e0" -Address "http://myServer.com/Citrix/sdkHostingUnitService"
```

Update the service instance with the unique identifier of '9805f39d-99eb-44f0-8f63-9d8e3f1228e0' to use the new address.

Set-ConfigRegisteredServiceInstanceMetadata

Sep 10, 2014

Adds or updates metadata on the given ServiceInstance.

Syntax

Set-ConfigRegisteredServiceInstanceMetadata [-ServiceInstanceUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigRegisteredServiceInstanceMetadata [-ServiceInstanceUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigRegisteredServiceInstanceMetadata [-InputObject] <ServiceInstance[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigRegisteredServiceInstanceMetadata [-InputObject] <ServiceInstance[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given ServiceInstance objects.

Related topics

Add-ConfigRegisteredServiceInstanceMetadata

Remove-ConfigRegisteredServiceInstanceMetadata

Parameters

-ServiceInstanceUid<Guid>

Id of the ServiceInstance

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<ServiceInstance[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the ServiceInstance specified. The property cannot contain any of the

following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-ConfigRegisteredServiceInstanceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- **EXAMPLE 1** ----------

```
c:\PS>Set-ConfigRegisteredServiceInstanceMetadata -ServiceInstanceUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

      Key                          Value
      ---                          -----
      property                       value
```

Add metadata with a name of 'property' and a value of 'value' to the ServiceInstance with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-ConfigServiceGroupMetadata

Sep 10, 2014

Adds or updates metadata on the given ServiceGroup.

Syntax

Set-ConfigServiceGroupMetadata [-ServiceGroupUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigServiceGroupMetadata [-ServiceGroupUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigServiceGroupMetadata [-InputObject] <ServiceGroup[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigServiceGroupMetadata [-InputObject] <ServiceGroup[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given ServiceGroup objects.

Related topics

Add-ConfigServiceGroupMetadata

Remove-ConfigServiceGroupMetadata

Parameters

-ServiceGroupUid<Guid>

Id of the ServiceGroup

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<ServiceGroup[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the ServiceGroup specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true

Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-ConfigServiceGroupMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Set-ConfigServiceGroupMetadata -ServiceGroupUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

    Key                            Value
    ---                            -----
    property                           value
```

Add metadata with a name of 'property' and a value of 'value' to the ServiceGroup with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-ConfigServiceMetadata

Sep 10, 2014

Adds or updates metadata on the given Service.

Syntax

Set-ConfigServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigServiceMetadata [-ServiceHostId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigServiceMetadata [-InputObject] <Service[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Allows you to store additional custom data against given Service objects.

Related topics

Remove-ConfigServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Service specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-ConfigServiceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------


```
c:\PS>Set-ConfigServiceMetadata -ServiceHostId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Service with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-ConfigSite

Sep 10, 2014

Changes the overall settings of the site.

Syntax

Set-ConfigSite [-SiteName <String>] [-ProductCode <String>] [-ProductEdition <String>] [-ProductVersion <String>] [-LicensingModel <String>] [-LicenseServerName <String>] [-LicenseServerPort <Int32>] [-LicenseServerUri <Uri>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-ConfigSite cmdlet modifies properties of the site.

The site is a top-level, logical representation of the XenDesktop site, from the perspective of the configuration services running within the site.

A XenDesktop installation has only a single site instance.

Modifications to the product code, product edition, product version and licensing model properties are successful only if their values are consistent with the feature table. Use the Get-ConfigProduct, Get-ConfigProductEdition, Get-ConfigProductVersion and Get-ConfigLicensingModel cmdlets to determine consistent values.

To configure the site, first import the feature table using the Import-ConfigFeatureTable cmdlet.

Related topics

Export-ConfigFeatureTable

Get-ConfigSite

Get-ConfigProduct

Get-ConfigProductEdition

Get-ConfigProductFeature

Get-ConfigProductVersion

Get-ConfigLicensingModel

Parameters

-SiteName<String>

Changes the name of the site.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ProductCode<String>

Changes the product code.

The Get-ConfigProduct cmdlet returns a list of supported values.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProductEdition<String>

Changes the license edition. A license matching the specified edition must be available within the site's license server.

The Get-ConfigProductEdition returns a list of supported values.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProductVersion<String>

Changes the product version.

The Get-ConfigProductVersion returns a list of supported values.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LicensingModel<String>

Changes the license model. A license matching the specified model must be available within the site's license server.

The Get-ConfigLicensingModel returns a list of supported values.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LicenseServerName<String>

Changes the machine used by the brokering services to obtain licenses for desktop and application session brokering. The specified machine must be running a Citrix license server and have suitable licenses installed.

The license server machine can be specified by its DNS name ('machine.domain') or its numeric IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LicenseServerPort<Int32>

Changes the port number on the license server machine used by the brokering services to contact the Citrix license server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LicenseServerUri<Uri>

Changes the Uri of the web server for licensing. The hostname component of this Uri must match the Site's LicenseServerName property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Site

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-ConfigSite -ProductEdition PLT
```

Specifies the use of a Platinum edition license. A suitable license must be available on the site's license server.

Set-ConfigSiteMetadata

Sep 10, 2014

Adds or updates metadata on the Site.

Syntax

```
Set-ConfigSiteMetadata -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ConfigSiteMetadata -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability for additional custom data to be stored against the Site.

Related topics

Remove-ConfigSiteMetadata

Parameters

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Site specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" =

"val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-ConfigSiteMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-ConfigSiteMetadata -Name property -Value value

        Key                         Value
```



```
---                             -----
property                        value
```

Add metadata with a name of 'property' and a value of 'value' to the Site.

Test-ConfigDBConnection

Sep 10, 2014

Tests a database connection for the Configuration Service.

Syntax

```
Test-ConfigDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Tests a connection to the database in which the Configuration Service can store its state. The service will attempt to connect to the database without affecting the current connection to the database.

You do not have to clear the connection to use this command.

Related topics

Get-ConfigServiceStatus

Get-ConfigDBConnection

Set-ConfigDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the Configuration Service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-ConfigDBConnection command returns an object containing the status of the Configuration Service if the connection string of the specified data store were to be set to the string being tested, together with extra diagnostics information for the specified connection string.

DBRejectedConnection

The database rejected the logon attempt from the Configuration Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Configuration Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Configuration Service currently in use is incompatible with the version of the Configuration Service schema on the database. Upgrade the Configuration Service to a more recent version.

DBOlderVersionThanService

The version of the Configuration Service schema on the database is incompatible with the version of the Configuration Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Set-ConfigDBConnection command would succeed if it were executed with the supplied connection string.

Failed

The Configuration Service has failed.

Unknown

The status of the Configuration Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Test-ConfigDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"
```


OK
Tests a database connection string for the Configuration Service.

---------- **EXAMPLE 2** ----------

c:\PS>Test-ConfigDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
Tests an invalid database connection string for the Configuration Service.

Test-ConfigServiceInstanceAvailability

Sep 10, 2014

Tests whether the supplied service instances are responding to requests.

Syntax

```
Test-ConfigServiceInstanceAvailability [-ServiceInstance] <ServiceInstance[]> [-MaxDelaySeconds <Int32>] [-ForceWaitForOneOfEachType] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Related topics

Register-ConfigServiceInstance

Unregister-ConfigRegisteredServiceInstance

Get-ConfigRegisteredServiceInstance

Parameters

-ServiceInstance<ServiceInstance[]>

The service instances to test.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-MaxDelaySeconds<Int32>

The timeout period to wait before concluding that services are unresponsive.

Required?	false
Default Value	Infinite
Accept Pipeline Input?	false

-ForceWaitForOneOfEachType<SwitchParameter>

If at least one of each type of service responds, finish immediately.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the host name or IP address of the controller to which the PowerShell snap-in connects.

Required?	false
Default Value	'LocalHost'. Once a value is specified by any command, this value becomes the new default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

This represents a service instance and has the following parameters;

ServiceGroupUid <Guid>

The unique identifer for the service group to which the service instance belongs.

ServiceGroupName <string>

The name of the service group that the service instance is part of.

ServiceInstanceUid <Guid>

The unique identifier for the service instance.

ServiceType <string>

The type of the service group.

Address <string>

The contact address for the service instance.

Binding <string>

The binding to use for connections to the service instance.

Version <int>

The version of the service instance.

ServiceAccount <string>

The AD computer account for the computer that is providing the service instance.

ServiceAccountSid <string>

The AD computer account SID for the computer that is providing the service instance.

InterfaceType <string>

The interface type for the service instance.

Metadata <Citrix.Configuration.Sdk.Metadata[]>

The metadata for the service instance.

Status <Citrix.Configuration.Sdk.Commands.Availability>

An enumeration value indicating whether the service is Responding, NotResponding, Unknown, or BadBindingType.

ResponseTime <System.TineSpan>

The interval elapsed between hailing the service and getting a definite response

Notes

The Availability Status Codes are o Responding: Got a positive response o NotResponding: Got a response, but it was negative or the connection was refused o Unknown: Did not respond in time / timed-out o BadBindingType: Binding parameter in ServiceInstance is not wcf_HTTP_kerb

Examples

---------- EXAMPLE 1 ----------

C:\>Get-ConfigRegisteredServiceInstance | Test-ConfigServiceInstanceAvailability -ForceWaitForOneOfEachType
Test all the service instances that are registered in the Configuration Service, returning when one of each type is responding.

---------- EXAMPLE 2 ----------

C:\>Test-ConfigServiceInstanceAvailability -ServiceInstance $services -MaxDelaySeconds 5
Test each of the given services, allowing a 5 second time-out.

Unregister-ConfigRegisteredServiceInstance

Sep 10, 2014

Removes a service instance from the Configuration Service registry.

Syntax

Unregister-ConfigRegisteredServiceInstance [-ServiceInstanceUid] <Guid> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Use this cmdlet to remove a service instance from the Configuration Service registry. This does not remove any service groups (if all service instances for a Service Group are removed, an empty service group remains and must be removed using the Remove-ConfigServiceGroup command).

Related topics

Register-ConfigServiceInstance

Parameters

-ServiceInstanceUid<Guid>

The unique identifier for the service instance to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the logging id of the high-level operation this cmdlet invocation is part of.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.Configuration.Sdk.ServiceInstance An object with a parameter called 'ServiceInstanceUid' can be used to unregister service instances.

Notes

In the case of failure, the following errors can result.

Error Codes ---------- ServiceInstanceObjectNotFound The service instance specified could not be located. DatabaseError An error occurred in the service while attempting a database operation. DatabaseNotConfigured The operation could not be completed because the database for the service is not configured. DataStoreException An error occurred in the service while attempting a database operation - communication with the database failed for various reasons. CommunicationError An error occurred while communicating with the service. ExceptionThrown An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

C:\PS>Get-ConfigRegisteredServiceInstance -ServiceType "Config" | Unregister-ConfigRegisteredServiceInstance
Unregisters all the service instances that are for a service type of 'Config' from the Configuration Service instance register.

Citrix.ConfigurationLogging.Admin.V1

Sep 10, 2014

Overview

Name	Description
LogConfigurationLoggingSnapin	The Configuration Logging Service PowerShell snap-in provides administrative
Log Filtering	Describes the common filtering options for XenDesktop cmdlets.
logical operators	Describes the operators that connect statements in Windows PowerShell.

Cmdlets

Name	Description
Export-LogReportCsv	Exports Configuration Logging data into a CSV file.
Export-LogReportHtml	Exports Configuration Logging data into a HTML report.
Get-LogDataStore	Gets details for each of the ConfigurationLogging data stores.
Get-LogDBConnection	Gets the database string for the specified data store used by the ConfigurationLogging Service.
Get-LogDBSchema	Gets a script that creates the ConfigurationLogging Service database schema for the specified data store.
Get-LogDBVersionChangeScript	Gets a script that updates the ConfigurationLogging Service database schema.
Get-LogHighLevelOperation	Gets high level operations
Get-LogInstalledDBVersion	Gets a list of all available database schema versions for the ConfigurationLogging Service.
Get-LogLowLevelOperation	Gets low level operations
Get-LogService	Gets the service record entries for the ConfigurationLogging Service.
Get-LogServiceAddedCapability	Gets any added capabilities for the ConfigurationLogging Service on the controller.

Name	Description
Get-LogServiceInstance	Gets the service instance entries for the ConfigurationLogging Service.
Get-LogServiceStatus	Gets the current status of the ConfigurationLogging Service on the controller.
Get-LogSite	Gets global configuration logging settings.
Get-LogSummary	Gets operations logged within time intervals inside a date range.
Remove-LogOperation	Deletes configuration logs
Remove-LogServiceMetadata	Removes metadata from the given Service.
Remove-LogSiteMetadata	Removes metadata from the given Site.
Reset-LogDataStore	Refreshes the database string currently being used by the Log service.
Reset-LogServiceGroupMembership	Reloads the access permissions and configuration service locations for the ConfigurationLogging Service.
Set-LogDBConnection	Configures a database connection for the ConfigurationLogging Service.
Set-LogServiceMetadata	Adds or updates metadata on the given Service.
Set-LogSite	Sets global configuration logging settings.
Set-LogSiteMetadata	Adds or updates metadata on the given Site.
Start-LogHighLevelOperation	Logs the start of a high level operation.
Stop-LogHighLevelOperation	Logs the completion of a previously started high level operation.
Test-LogDBConnection	Tests a database connection for the ConfigurationLogging Service.

about_LogConfigurationLoggingSnapin

Sep 10, 2014

TOPIC

about_LogConfigurationLoggingSnapin

SHORT DESCRIPTION

The Configuration Logging Service PowerShell snap-in provides administrative functions for the Configuration Logging Service.

COMMAND PREFIX

All commands in this snap-in have the noun prefixed with 'Log'.

LONG DESCRIPTION

The Configuration Logging Service PowerShell snap-in enables both local and remote administration of the Configuration Logging Service.

The Configuration Logging Service logs configuration changes or administrator requested state changes made to the site. Configuration Logging can be configured, site wide, to be mandatory or optional. If mandatory logging is selected, then any attempts to change site configuration or state when the logging mechanism is unavailable are denied.

The Configuration Logging Service stores information about the logged changes in a database which can be configured to be separate from the site database.

The snap-in provides storage and configuration of these entities:

Site

> The Configuration Logging Site object holds global settings which control the behaviour of the Configuration Logging Service. The site object can be configured by the Set-LogSite cmdlet. The properties of the site object are returned by the Get-LogSite cmdlet.

High Level Operations

> A high level operation object represents a logged configuration change performed from Desktop Studio, Desktop Director or a PowerShell Script.
>
> The XenDesktop consoles log high level operations when:
>
> 1) Executing operations which performs configuration changes.
> 2) Executing operations which performs administration related activities which may affect site configuration.

PowerShell scripts which carry out customized configuration changes can also log high level operations via cmdlets Start-LogHighLevelOperation and Stop-LogHighLevelOperation.

Low Level Operations

A low level operation object represents a logged configuration change performed by a service. One or more low level operation objects are used to record the actions performed by a services in order to fulfil a high level operation initiated from the consoles, or from PowerShell scripts.

Low level operations in the system are returned by cmdlet Get-LogLowLevelOperation.

Operation Details

A low level operation performed by a service can affect a number of individual objects, or a number of properties on an object. An operation detail log records each individual change to an object. This includes the creation and deletion of the object, as well as changes to individual properties of the object.

One or more operation detail objects are used to record specific changes to each object that is affected by a low level service operation.

Operation details are included in the data returned from the Get-LogLowLevelOperation cmdlet.

High Level Operations, Low Level Operations and Operation Details are arranged in a hierarchy. A High Level Operation can have multiple Low Level Operations, and each Low Level Operation can have multiple Operation Details.

Setting up a separate logging database ---------- After creating the database on the database server, the logging database can be setup and configured for use by:

1) Generating the database schema, and applying it the logging database
2) Configuring the configuration logging service to use the new logging database.

The logging database schema can be generated from the Get-LogDBSchem cmdlet, as illustrated below:

```
Get-LogDBSchema -DatabaseName "loggingDB"
                -ServiceGroupName "service group name"
                -ScriptType Database
                -LocalDatabase:$LocalDB
                -DataStore Logging
```

The configuration logging service can be configured to use the logging database with the Set-LogDBConnection cmdlet, as illustrated below:

```
Set-LogDBConnection -DataStore Logging -DBConnection $null
Set-LogDBConnection -DataStore Logging -DBConnection "new logging db connection string"
```

Configuration Logging site settings ----------

On the Site object:

- The 'State' setting allows configuration logging to be disabled, enabled, or made mandatory.
- The 'Locale' setting specifies the language in which configuration logging data text will be stored.

See Get-LogSite cmdlet help for further information on these settings.

This locale setting applies to the text description that is associated with each log , e.g. "Create Catalog". It doesn't apply to other textual information in the log like the names of parameters passed to operations, e.g. "CatalogName".

This localisation is applied when the data is logged, and not when the logs are viewed later. For example, logs which are created in English will be displayed in English on an end user system which may be configured with a different locale.

about_Log_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```

retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

```
A120901
B220000
...
```

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

about_logical_operators

Sep 10, 2014

TOPIC

about_Logical_Operators

SHORT DESCRIPTION

Describes the operators that connect statements in Windows PowerShell.

LONG DESCRIPTION

The Windows PowerShell logical operators connect expressions and statements, allowing you to use a single expression to test for multiple conditions.

For example, the following statement uses the and operator and the or operator to connect three conditional statements. The statement is true only when the value of $a is greater than the value of $b, and either $a or $b is less than 20.

```
($a -gt $b) -and (($a -lt 20) -or ($b -lt 20))
```

Windows PowerShell supports the following logical operators.

```
Operator  Description                  Example
--------  -----------------------------  ------------------------
-and      Logical and. TRUE only when    (1 -eq 1) -and (1 -eq 2)
          both statements are TRUE.      False

-or       Logical or. TRUE when either   (1 -eq 1) -or (1 -eq 2)
          or both statements are TRUE.   True

-xor      Logical exclusive or. TRUE     (1 -eq 1) -xor (2 -eq 2)
          only when one of the statements False
          is TRUE and the other is FALSE.

-not      Logical not. Negates the       -not (1 -eq 1)
          statement that follows it.     False

!         Logical not. Negates the       !(1 -eq 1)
          statement that follows it.     False
          (Same as -not)
```

Note: The previous examples also use the equal to comparison

operator (-eq). For more information, see about_Comparison_Operators. The examples also use the Boolean values of integers. The integer 0 has a value of FALSE. All other integers have a value of TRUE.

The syntax of the logical operators is as follows:

```
<statement> {-AND | -OR | -XOR} <statement>
{! | -NOT} <statement>
```

Statements that use the logical operators return Boolean (TRUE or FALSE) values.

The Windows PowerShell logical operators evaluate only the statements required to determine the truth value of the statement. If the left operand in a statement that contains the and operator is FALSE, the right operand is not evaluated. If the left operand in a statement that contains the or statement is TRUE, the right operand is not evaluated. As a result, you can use these statements in the same way that you would use the If statement.

SEE ALSO

about_Operators

Compare-Object

about_Comparison_operators

about_If

Export-LogReportCsv

Sep 10, 2014

Exports Configuration Logging data into a CSV file.

Syntax

```
Export-LogReportCsv -OutputFile <String> [-StartDateRange <DateTime>] [-EndDateRange <DateTime>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This cmdlet exports the Configuration Logging data into a CSV data file. The hierarchical logging data is flattened into a single CSV 'table'. The content of CSV file is not intended to be human-readable. It is meant to be input data for external reporting or manipulation tools (for example, a spread sheet application).

Related topics

Export-LogReportHtml

Parameters

-OutputFile<String>

Specifies the path to a file where the CSV data will be saved.

Required?	true
Default Value	
Accept Pipeline Input?	false

-StartDateRange<DateTime>

Specifies the start time of the earliest operation to include.

Required?	false
Default Value	DateTime.Min
Accept Pipeline Input?	false

-EndDateRange<DateTime>

Specifies the end time of the latest operation to include.

Required?	false
Default Value	DateTime.UtcNow
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Examples

-------------------------- EXAMPLE 1 --------------------------

C:\PS> Export-LogReportCsv -OutputFile "c:\MyReports\LoggingData.csv"
Export all logged operations to a csv file.

-------------------------- EXAMPLE 2 --------------------------

C:\PS> Export-LogReportCsv -OutputFile "c:\MyReports\LoggingData.csv" -StartDateRange "2012-12-21 09:00"
Export to a CSV file logged operations started on or after a specified datetime..

-------------------------- EXAMPLE 3 --------------------------

C:\PS> Export-LogReportCsv -OutputFile "c:\MyReports\LoggingData.csv" -StartDateRange "2012-12-21 09:00" -EndDateRange "2012-12-311 18:00"
Export to a CSV file logged operations started and completed between a date range.

Export-LogReportHtml

Sep 10, 2014

Exports Configuration Logging data into a HTML report.

Syntax

```
Export-LogReportHtml -OutputDirectory <String> [-StartDateRange <DateTime>] [-EndDateRange <DateTime>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This cmdlet exports the Configuration Logging data into a HTML report. The report consists of two HTML files:

o Summary.Html - this shows summary information from the high level operation logs.

o Details.Html - this shows additional logging data from the low level operation and operation detail logs.

Hyperlinks in summary.html allow drill-down into the associated low level logging data contained within details.html.

Related topics

Export-LogReportCsv

Parameters

-OutputDirectory<String>

Specifies the path to a directory where the HTML report files will will be saved.

Required?	true
Default Value	
Accept Pipeline Input?	false

-StartDateRange<DateTime>

Specifies the start time of the earliest operation to include.

Required?	false
Default Value	DateTime.Min
Accept Pipeline Input?	false

-EndDateRange<DateTime>

Specifies the end time of the latest operation to include.

Required?	false
Default Value	DateTime.UtcNow
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Examples

---------- EXAMPLE 1 ----------

C:\PS> Export-LogReportHtml -OutputDirectory "c:\MyReports"
Export all logged operations to HTML.

---------- EXAMPLE 2 ----------

C:\PS> Export-LogReportHtml -OutputDirectory "c:\MyReports" -StartDateRange "2012-12-21 09:00"
Export to a HTML logged operations started on or after a specified datetime..

---------- EXAMPLE 3 ----------

C:\PS> Export-LogReportHtml -OutputDirectory "c:\MyReports" -StartDateRange "2012-12-21 09:00" -EndDateRange "2012-12-311 18:00"
Export to HTML logged operations started and completed between a date range.

Get-LogDataStore

Sep 10, 2014

Gets details for each of the ConfigurationLogging data stores.

Syntax

```
Get-LogDataStore [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns an object for each of the ConfigurationLogging data stores describing the connection string, data store name, db type, provider, schema name, and DB status.

A database connection must be configured in order for this command to be used if the service has a secondary data store. This is not required for the site data store.

Related topics

Reset-LogDataStore

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.ConfigurationLogging.Sdk.DataStoreConfiguration

An object describing the connection string, data store name, database type, provider, schema name and database status.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-LogDataStore

ConnectionString : Server=.\SQLEXPRESS;Initial Catalog = databaseName; Integrated Security = True
DataStore        : Site
DatabaseType     : SqlServer
Provider         : MSSQL
SchemaName       : LogSiteSchema
Status           : OK

ConnectionString :
DataStore        : Secondary
DatabaseType     : SqlServer
Provider         : MSSQL
SchemaName       : LogSecondarySchema
Status           : DBUnconfigured
```

Get the database connection string for the ConfigurationLogging Service.

Get-LogDBConnection

Sep 10, 2014

Gets the database string for the specified data store used by the ConfigurationLogging Service.

Syntax

```
Get-LogDBConnection [[-DataStore] <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the database connection string for the specified data store.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

Related topics

Get-LogServiceStatus

Get-LogDataStore

Set-LogDBConnection

Test-LogDBConnection

Parameters

-DataStore<String>

Specifies the logical name of the data store for the ConfigurationLogging Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false
Default Value	Site
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

system.string

The database connection string configured for the ConfigurationLogging Service.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the ConfigurationLogging Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-LogDBConnection

Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True
```


Get the database connection string for the ConfigurationLogging Service.

Get-LogDBSchema

Sep 10, 2014

Gets a script that creates the ConfigurationLogging Service database schema for the specified data store.

Syntax

```
Get-LogDBSchema [-DatabaseName <String>] [-ServiceGroupName <String>] [-ScriptType <ScriptTypes>] [-LocalDatabase] [-Sid <String>] [-DataStore <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets SQL scripts that can be used to create a new ConfigurationLogging Service database schema, add a new ConfigurationLogging Service to an existing site, remove a ConfigurationLogging Service from a site, or create a database server logon for a ConfigurationLogging Service. If no Sid parameter is provided, the scripts obtained relate to the currently selected ConfigurationLogging Service instance, otherwise the scripts relate to ConfigurationLogging Service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied. The current service instance is that on the local machine, or that explicitly specified by the last usage of the -AdminAddress parameter to a ConfigurationLogging SDK cmdlet. The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured. The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SMDCMD mode'. The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to ConfigurationLogging Service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to ConfigurationLogging Service roles

If ScriptType is Evict, the returned script contains:

o Removal of ConfigurationLogging Service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database. You do not need to configure a database before using this command.

Related topics

Get-LogDataStore

Set-LogDBConnection

Parameters

-DatabaseName<String>

Specifies the name of the database for which the schema will be generated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the ConfigurationLogging services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<ScriptTypes>

Specifies the type of database script returned. Available script types are:

Database

Returns a full database script that can be used to create a database schema for the ConfigurationLogging Service in a database instance that does not already contain a schema for this service. The DatabaseName and ServiceGroupName parameters must be specified to create a script of this type.

Instance

Returns a permissions script that can be used to add further ConfigurationLogging services to an existing database instance that already contains the full ConfigurationLogging service schema, associating the services to the Service Group. The Sid parameter can optionally be specified to create a script of this type.

Login

Returns a database logon script that can be used to add the required logon accounts to an existing database instance that contains the ConfigurationLogging Service schema. This is used primarily when creating a mirrored database environment. The DatabaseName parameter must be specified to create a script of this type.

Evict

Returns a script that can be used to remove the specified ConfigurationLogging Service from the database entirely. The DatabaseName and Sid parameters must be specified to create a script of this type.

Required?	false
Default Value	Database
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for

ConfigurationLogging services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Sid<String>

Specifies the SID of the controller on which the ConfigurationLogging Service instance to remove from the database is running.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-DataStore<String>

Specifies the logical name of the data store for the ConfigurationLogging Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false
Default Value	Site
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.string

A string containing the required SQL script for application to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-LogDBSchema -DatabaseName MyDB -ServiceGroupName  MyServiceGroup > c:\LogSchema.sql
```

Get the full database schema for site data store of the ConfigurationLogging Service and copy it to a file called 'c:\LogSchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a ConfigurationLogging Service site schema.

---------- EXAMPLE 2 ----------

c:\PS>Get-LogDBSchema -DatabaseName MyDB -scriptType Login > c:\ConfigurationLoggingLogins.sql
Get the logon scripts for the ConfigurationLogging Service.

---------- EXAMPLE 3 ----------

c:\PS>Get-LogDBSchema -DatabaseName MyDB -ServiceGroupName MyServiceGroup -DataStore Secondary > c:\LogSchema.sql
Get the full database schema for the secondary data store of the ConfigurationLogging Service and copy it to a file called 'c:\LogSecondarySchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a ConfigurationLogging Service secondary schema.

Get-LogDBVersionChangeScript

Sep 10, 2014

Gets a script that updates the ConfigurationLogging Service database schema.

Syntax

```
Get-LogDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-DataStore <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a database script that can be used to upgrade or downgrade the site or secondary schema for the ConfigurationLogging Service from the current schema version to a different version.

Related topics

Get-LogInstalledDBVersion

Parameters

-DatabaseName<String>

Specifies the name of the database instance to which the update applies.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

Specifies the version of the database you want to update to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-DataStore<String>

Specifies the logical name of the data store for the ConfigurationLogging Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false
Default Value	Site
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

A PSObject containing the required SQL script for application to a database.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any ConfigurationLogging services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-LogServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the ConfigurationLogging Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS> $update = Get-LogDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-LogHighLevelOperation

Sep 10, 2014

Gets high level operations

Syntax

```
Get-LogHighLevelOperation [-Id <Guid>] [-Text <String>] [-StartTime <DateTime>] [-Source <String>] [-EndTime <DateTime>] [-IsSuccessful <Boolean>] [-User <String>] [-AdminMachineIP <String>] [-OperationType <OperationType>] [-TargetType <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Retrieves high level operations matching the specified criteria. If no parameters are specified this cmdlet returns all high level operations.

Related topics

Start-LogHighLevelOperation

Stop-LogHighLevelOperation

Get-LogLowLevelOperation

Parameters

-Id<Guid>

Gets the high level operation with the specified identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Text<String>

Gets high level operations with the specified text

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartTime<DateTime>

Gets high level operations with the specified start time

Required?	false
Default Value	

Accept Pipeline Input?	false

-Source<String>

Gets high level operations with the specified source.

Required?	false
Default Value	
Accept Pipeline Input?	false

-EndTime<DateTime>

Gets high level operations with the specified end time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsSuccessful<Boolean>

Gets high level operations with the specified success indicator.

Required?	false
Default Value	
Accept Pipeline Input?	false

-User<String>

Gets high level operations logged by the specified user.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminMachineIP<String>

Gets high level operations logged from the machine with the specified IP address.

Required?	false

Default Value	
Accept Pipeline Input?	false

-OperationType<OperationType>

Gets high level operations with the specified operation type. Values can be:

o AdminActivity - to get operations which log administration activity.

o ConfigurationChange - to get operations which log configuration changes.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TargetType<String>

Gets high level operations with the specified target type. The target type describes the type of object that was the target of the configuration change. For example, "Session" or "Machine".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Log_Filtering for details.

Required?	false
Default Value	False

Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Log_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.ConfigurationLogging.Sdk.HighLevelOperation

The returned HighLevelOperation object has the following properties:

o Id - The unique identifier of the operation.

o Text - A description of the operation.

o StartTime - The date and time that the operation started.

o EndTime - The date and time that the operation completed. This will be null if the operation is still in progress, or if the operation never completed.

o IsSuccessful - Indicates whether the operation completed successfully or not. This will be null if the operation is still in progress, or if the operation never completed.

o User - The identifier of the administrator who performed the operation.

o AdminMachineIP - The IP address of the machine that the operation was initiated from.

o Source - Identifies the XenDesktop console, or custom script, where the operation was initiated from. For example, "Desktop Studio", "Desktop Director", "My custom script".

o OperationType - The operation type. This can be 'AdminActivity' or 'ConfigurationChange'.

o TargetTypes - Identifies the type of objects that were affected by the operation. For example, "Catalog" or "Desktop","Machine".

o Parameters - The names and values of the parameters that were supplied for the operation.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Get-LogHighLevelOperation
Get all high level operations

---------- EXAMPLE 2 ----------

C:\PS> Get-LogHighLevelOperation -OperationType ConfigurationChange
Get high level operations which log configuration changes.

---------- EXAMPLE 3 ----------

C:\PS> Get-LogHighLevelOperation -OperationType AdminActivity
Get high level operations which log administration activities.

---------- EXAMPLE 4 ----------

C:\PS> Get-LogHighLevelOperation -Filter{ StartTime -ge "2013-02-27 09:00:00" -and EndTime -le "2013-02-27 18:00:00"}
Use advanced filtering to get high level operations with a start time on or after "2013-02-27 09:00:00" and an end time on or before "2013-02-27 18:00:00".

---------- EXAMPLE 5 ----------

```
C:\PS> Get-LogHighLevelOperation -EndTime $null
C:\PS> Get-LogHighLevelOperation -IsSuccessful $null
```

Either of these commands will get high level operations which have not yet been completed.

---------- EXAMPLE 6 ----------

```
C:\PS> Get-LogHighLevelOperation -User "DOMAIN\UserName"
```

Get high level operations performed by user "DOMAIN\UserName".

Get-LogInstalledDBVersion

Sep 10, 2014

Gets a list of all available database schema versions for the ConfigurationLogging Service.

Syntax

```
Get-LogInstalledDBVersion [-Upgrade] [-Downgrade] [-DataStore <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the current version of the ConfigurationLogging Service database schema, if no flags are set, otherwise returns versions for which upgrade or downgrade scripts are available and have been stored in the database.

Related topics

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DataStore<String>

Specifies the database connection logical name the schema script should be returned for. The parameter is optional.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Version

The Get-LogInstalledDbVersion command returns objects containing the new definition of the ConfigurationLogging Service database schema version.

Major <Integer>

Minor <Integer>

Build <Integer>

Revision <Integer>

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the ConfigurationLogging Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-LogInstalledDBVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      6      0      0
```

Get the currently installed version of the ConfigurationLogging Service database schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-LogInstalledDBVersion -Upgrade

Major  Minor  Build  Revision
-----  -----  -----  --------
6      0      0      0
```

Get the versions of the ConfigurationLogging Service database schema for which upgrade scripts are supplied.

Get-LogLowLevelOperation

Sep 10, 2014

Gets low level operations

Syntax

```
Get-LogLowLevelOperation [-Id <Guid>] [-HighLevelOperationId <Guid>] [-StartTime <DateTime>] [-EndTime <DateTime>] [-IsSuccessful <Boolean>] [-User <String>] [-AdminMachineIP <String>] [-Text <String>] [-Source <String>] [-SourceSdk <String>] [-OperationType <OperationType>] [-TargetType <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Retrieves low level operations matching the specified criteria. If no parameters are specified this cmdlet returns all low level operations.

Related topics

Get-LogLowLevelOperation

Parameters

-Id<Guid>

Gets the low level operation with the specified identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-HighLevelOperationId<Guid>

Gets low level operations for the high level operation with the specified identifier.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartTime<DateTime>

Gets low level operations with the specified start time

Required?	false
Default Value	
Accept Pipeline Input?	false

-EndTime<DateTime>

Gets low level operations with the specified end time.

Required?	false
Default Value	
Accept Pipeline Input?	false

-IsSuccessful<Boolean>

Gets low level operations with the specified success indicator.

Required?	false
Default Value	
Accept Pipeline Input?	false

-User<String>

Gets low level operations logged by the specified administrator.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminMachineIP<String>

Gets low level operations logged from the machine with the specified IP address.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Text<String>

Gets low level operations with the specified text

Required?	false
Default Value	

Accept Pipeline Input?	false

-Source<String>

Gets low level operations with the specified source.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SourceSdk<String>

Gets low level operations logged from the SDK with the specified identifier.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OperationType<OperationType>

Gets low level operations with the specified operation type. Values can be:

o AdminActivity - to get operations which log administration activity.

o ConfigurationChange - to get operations which log configuration changes.

Required?	false
Default Value	
Accept Pipeline Input?	false

-TargetType<String>

Gets low level operations with the specified target type. The target type describes the type of object that was the target of the configuration change. For example, "Session" or "Machine".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Log_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false

Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Log_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.ConfigurationLogging.Sdk.LowLevelOperation

The returned LowLevelOperation object has the following properties:

o Id - The unique identifier of the operation.

o Text - A description of the operation.

o HighLevelOperationId - The unique identifier of the related high level operation.

o StartTime - The date and time that the operation started.

o EndTime - The date and time that the operation completed. This will be null if the operation is still in progress, or if the operation never completed.

o IsSuccessful - Indicates whether the operation completed successfully or not. This will be null if the operation is still in progress, or if the operation never completed.

o AdminSid - The identifier of the administrator who performed the operation.

o AdminMachineIP - The IP address of the machine that the operation was performed on.

o Source - The name of the XenDesktop service that the operation was performed on; for example, "MachineCreation", "DelegatedAdmin".

o SourceSdk - The identifier of the XenDesktop service SDK through which the operation was performed; for example, "Prov", "Admin".

o OperationType - The operation type. This can be 'AdminActivity' or 'ConfigurationChange'.

o TargetTypes - Identifies the type of objects that were affected by the operation. For example, "Catalog" or "Desktop","Machine".

o Parameters - The names and values of the parameters that were supplied for the operation.

o Details - A collection of OperationDetail objects containing specific information about each object affected by the operation.

Each OperationDetail object in the 'Details' collection has the following properties:

o TargetUid - The unique identifier of the target object affected by the operation.

o TargetName - The name of the target object affected by the operation.

o TargetType - The type of the target object.

o Text - The description of operation performed on the target object.

o StartTime - The date and time that the operation started.

o EndTime - The date and time that the operation completed. This will be null if the operation is still in progress, or if the operation never completed.

o IsSuccessful - Indicates whether the operation completed successfully or not. This will be null if the operation is still in progress, or if the operation didn't complete.

The following properties will be set if the operation changed a property on the object:

o PropertyName - The name of the changed property.

o NewValue - The new property value.

o PreviousValue - The previous property value.

o AddValue - If the object property contains a set of values, this specifies the new value which was added to the set.

o RemoveValue- If the object property contains a set of values, this specifies the value which was removed from the set.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-LogLowLevelOperation
```

Get all low level operations

---------- EXAMPLE 2 ----------

```
C:\PS> Get-LogLowLevelOperation -OperationType ConfigurationChange
```

Get low level operations which log configuration changes.

---------- EXAMPLE 3 ----------

```
C:\PS> Get-LogLowLevelOperation -OperationType AdminActivity
```

Get low level operations which log administration activities.

---------- EXAMPLE 4 ----------

```
C:\PS> Get-LogLowLevelOperation -Filter{ StartTime -ge "2013-02-27 09:00:00" -and EndTime -le "2013-02-27 18:00:00"}
```

Use advanced filtering to get low level operations with a start time on or after "2013-02-27 09:00:00" and an end time on or before "2013-02-27 18:00:00".

---------- EXAMPLE 5 ----------

```
C:\PS> Get-LogLowLevelOperation -EndTime $null
C:\PS> Get-LogLowLevelOperation -IsSuccessful $null
```


Either of these commands will get low level operations which have not yet been completed.

---------- **EXAMPLE 6** ----------

```
C:\PS> Get-LogLowLevelOperation -User "DOMAIN\UserName"
```

Get low level operations performed by user "DOMAIN\UserName".

Get-LogService

Sep 10, 2014

Gets the service record entries for the ConfigurationLogging Service.

Syntax

Get-LogService [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns instances of the ConfigurationLogging Service that the service publishes. The service records contain account security identifier information that can be used to remove each service from the database.

A database connection for the service is required to use this command.

Related topics

Parameters

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Log_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Log_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.ConfigurationLogging.Sdk.Service

The Get-LogServiceInstance command returns an object containing the following properties.

Uid <Integer>

Specifies the unique identifier for the service in the group. The unique identifier is an index number.

ServiceHostId <Guid>

Specifies the unique identifier for the service instance.

DNSName <String>

Specifies the domain name of the host on which the service runs.

MachineName <String>

Specifies the short name of the host on which the service runs.

CurrentState <Citrix.Fma.Sdk.ServiceCore.ServiceState>

Specifies whether the service is running, started but inactive, stopped, or failed.

LastStartTime <DateTime>

Specifies the date and time at which the service was last restarted.

LastActivityTime <DateTime>

Specifies the date and time at which the service was last stopped or restarted.

OSType

Specifies the operating system installed on the host on which the service runs.

OSVersion

Specifies the version of the operating system installed on the host on which the service runs.

ServiceVersion

Specifies the version number of the service instance. The version number is a string that reflects the full build version of the service.

DatabaseUserName <string>

Specifies for the service instance the Active Directory account name with permissions to access the database. This will be either the machine account or, if the database is running on a controller, the NetworkService account.

Sid <string>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

ActiveSiteServices <string[]>

Specifies the names of active site services currently running in the service. Site services are components that perform long-running background processing in some services. This field is empty for services that do not contain site services.

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-LogService

Uid             : 1
ServiceHostId     : aef6f464-f1ee-4042-a523-66982e0cecd0
DNSName           : MyServer.company.com
MachineName       : MYSERVER
CurrentState      : On
LastStartTime     : 04/04/2011 15:25:38
LastActivityTime  : 04/04/2011 15:33:39
OSType            : Win32NT
OSVersion         : 6.1.7600.0
ServiceVersion    : 5.1.0.0
DatabaseUserName  : NT AUTHORITY\NETWORK SERVICE
SID               : S-1-5-21-2316621082-1546847349-2782505528-1165
ActiveSiteServices : {MySiteService1, MySiteService2...}
```

Get all the instances of the ConfigurationLogging Service running in the current service group.

Get-LogServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the ConfigurationLogging Service on the controller.

Syntax

```
Get-LogServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the ConfigurationLogging Service on the controller to be detected.

You do not need to configure a database connection before using this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-LogServiceAddedCapability
```

Get the added capabilities of the ConfigurationLogging Service.

Get-LogServiceInstance

Sep 10, 2014

Gets the service instance entries for the ConfigurationLogging Service.

Syntax

```
Get-LogServiceInstance [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns service interfaces published by the instance of the ConfigurationLogging Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.ConfigurationLogging.Sdk.ServiceInstance

The Get-LogServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a

central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

Specifies the service instance type. For this service, the service instance type is always Log.

Address

Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

SDK - for PowerShell operations

InterService - for operations between different services

Peer - for communications between services of the same type

Metadata <Citrix.ConfigurationLogging.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-LogServiceInstance

Address          : http://MyServer.com:80/Citrix/ConfigurationLoggingService
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         :
MetadataMap      :
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName  : MyServiceGroup
ServiceGroupUid   : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType      : Log
Version          : 1

Address          : http://MyServer.com:80/Citrix/ConfigurationLoggingService/IServiceApi
Binding          : wcf_HTTP_kerb
InterfaceType    : InterService
Metadata         :
MetadataMap      :
```



```
ServiceAccount     : ENG\MyAccount
ServiceAccountSid  : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName   : MyServiceGroup
ServiceGroupUid    : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType        : Log
Version            : 1
```

Get all instances of the ConfigurationLogging Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-LogServiceStatus

Sep 10, 2014

Gets the current status of the ConfigurationLogging Service on the controller.

Syntax

```
Get-LogServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the ConfigurationLogging Service on the controller to be monitored. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured.

Related topics

Get-LogDataStore

Set-LogDBConnection

Test-LogDBConnection

Get-LogDBConnection

Get-LogDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-LogServiceStatus command returns an object containing the status of the ConfigurationLogging Service together with extra diagnostics information.

DBUnconfigured

The ConfigurationLogging Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the ConfigurationLogging Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the ConfigurationLogging Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the ConfigurationLogging Service currently in use is incompatible with the version of the ConfigurationLogging Service schema on the database. Upgrade the ConfigurationLogging Service to a more recent version.

DBOlderVersionThanService

The version of the ConfigurationLogging Service schema on the database is incompatible with the version of the ConfigurationLogging Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The ConfigurationLogging Service is running and is connected to a database containing a valid schema.

Failed

The ConfigurationLogging Service has failed.

Unknown

(0) The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-LogServiceStatus

DBUnconfigured
```

Get the current status of the ConfigurationLogging Service.

Get-LogSite

Sep 10, 2014

Gets global configuration logging settings.

Syntax

```
Get-LogSite [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This cmdlet retrieves the global configuration logging settings.

Related topics

Set-LogSite

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.ConfigurationLogging.Sdk.Site

Get-LogSite returns an object containing the following properties:

o Locale - the current language that logs should be recorded in. Can be: 'en', 'ja', 'zh-CN', 'de', 'es' or 'fr'.

o State - the current state of configuration logging. Can be: Enabled, Disabled, Mandatory or NotSupported.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-LogSite
```

Gets configiration logging site settings.

Get-LogSummary

Sep 10, 2014

Gets operations logged within time intervals inside a date range.

Syntax

```
Get-LogSummary [-StartDateRange <DateTime>] [-EndDateRange <DateTime>] [-IntervalSeconds <Int64>] [-GetLowLevelOperations] [-IncludeIncomplete] [-OperationType <OperationType>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Get-LogSummary cmdlet retrieves summary counts of operations logged within time intervals inside a date range. The returned data indicates the rate at which configuration changes and activities were performed out within a time period.

Related topics

Get-LogHighLevelOperation

Get-LogLowLevelOperation

Parameters

-StartDateRange<DateTime>

Specifies the start of the summary period date range

Required?	false
Default Value	1900-01-01 00:00:00
Accept Pipeline Input?	false

-EndDateRange<DateTime>

Specifies the end of the summary period date range.

Required?	false
Default Value	DateTime.UtcNow
Accept Pipeline Input?	false

-IntervalSeconds<Int64>

Specifies the size, in seconds, of each time interval required within the summary date range. If this is not specified, is null, zero or exceeds the specified date range, it defaults to the total number of seconds between EndDateRange and StartDateRange.

Required?	false
Default Value	Total number of seconds in the EndDateRange and StartDateRange time span.
Accept Pipeline Input?	false

-GetLowLevelOperations<SwitchParameter>

Specifies if the cmdlet should return low level operation summary counts.

Required?	false
Default Value	$false - high level operations counts are returned.
Accept Pipeline Input?	false

-IncludeIncomplete<SwitchParameter>

Specifies if incomplete operations should be included in the returned summary counts.

Required?	false
Default Value	$false - incomplete operations are excluded.
Accept Pipeline Input?	false

-OperationType<OperationType>

Specifies the type of logged operations to include. Values can be 'AdminActivity' or 'ConfigurationChange'

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary<string, int>

The summary data is returned as a collection of dictionary items. The 'Key' value of each dictionary item specifies the start of the time interval within the overall summary date range. The 'Value' data in each dictionary item contains the count of operations which were started within that time interval.

Notes

If the specified summary date range and interval period will result in more than 50,000 intervals being returned Get-LogSummary will generate an error and abort the operation.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $logSummary = Get-LogSummary
```

Get a summary of all completed high level operations. The returned log summary collection will contain a single item for the time period spanning the entire [1900-01-01 00:00:00]-[UtcNow] date range. e.g.

Key ==> Value

01/01/1900 00:00:00 ==> 41

---------- EXAMPLE 2 ----------

```
C:\PS> $daily = 60*60*24
C:\PS> [DateTime]$startRange = "2013-02-01 14:50:39"
C:\PS> [DateTime]$endRange = $startRange.AddDays(14)
C:\PS> Get-LogSummary -StartDateRange $startRange -EndDateRange $endRange -intervalSeconds $daily
```

Gets a summarised count of completed high level operations logged over two weeks, at daily intervals. The returned log summary collection will contain multiple items; one for each day in the summary date range. - e.g.

Key ==> Value

01/02/2013 14:50:39 ==> 0

02/02/2013 14:50:39 ==> 4

03/02/2013 14:50:39 ==> 21

04/02/2013 14:50:39 ==> 0

05/02/2013 14:50:39 ==> 0

06/02/2013 14:50:39 ==> 0

07/02/2013 14:50:39 ==> 5

08/02/2013 14:50:39 ==> 0

09/02/2013 14:50:39 ==> 0

10/02/2013 14:50:39 ==> 0

11/02/2013 14:50:39 ==> 0

12/02/2013 14:50:39 ==> 7

13/02/2013 14:50:39 ==> 0

14/02/2013 14:50:39 ==> 0

15/02/2013 14:50:39 ==> 12

---------- EXAMPLE 3 ----------

```
C:\PS> $hourly = 60*60
C:\PS> [DateTime]$startRange = "2013-02-03 00:00:00"
C:\PS> [DateTime]$endRange = "2013-02-03 23:59:59"
C:\PS> Get-LogSummary -StartDateRange $startRange -EndDateRange $endRange -intervalSeconds $hourly -GetLowLevelOperations
```

Gets a summarised count of completed low level operations logged during a day, at hourly intervals. The returned log summary collection will contain multiple items; one for each hour in the summary date range - e.g.

Key ==> Value

04/03/2013 00:00:00 ==> 12

04/03/2013 01:00:00 ==> 10

04/03/2013 02:00:00 ==> 5

.

.

.

04/03/2013 21:00:00 ==> 26

04/03/2013 22:00:00 ==> 0

04/03/2013 23:00:00 ==> 9

Remove-LogOperation

Sep 10, 2014

Deletes configuration logs

Syntax

Remove-LogOperation -DatabaseCredentials <PSCredential> [-StartDateRange <DateTime>] [-EndDateRange <DateTime>] [-IncludeIncomplete] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-LogOperation -UserName <String> [-Password <String>] [-StartDateRange <DateTime>] [-EndDateRange <DateTime>] [-IncludeIncomplete] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-LogOperation -UserName <String> -SecurePassword <SecureString> [-StartDateRange <DateTime>] [-EndDateRange <DateTime>] [-IncludeIncomplete] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Remove-LogOperation deletes logs from the Configuration Logging database. This cmdlet targets high level operation logs for deletion. The associated low level operations logs are deleted as part of this operation via cascade deletion functionality present in the configuration logging database schema.

Related topics

Parameters

-DatabaseCredentials<PSCredential>

Specifies the credentials of a database user with permission to delete records from the Configuration Logging database.

Required?	true
Default Value	
Accept Pipeline Input?	false

-UserName<String>

Specifies the user name of a database user with permission to delete records from the Configuration Logging database.

Required?	true
Default Value	
Accept Pipeline Input?	false

-SecurePassword<SecureString>

Specifies the password a database user, in secure string form, with permission to delete records from the Configuration Logging database.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Password<String>

Specifies the password of a database user with permission to delete records from the Configuration Logging database.

Required?	false
Default Value	
Accept Pipeline Input?	false

-StartDateRange<DateTime>

Specifies the start time of the earliest high level operation to delete

Required?	false
Default Value	DateTime.Min
Accept Pipeline Input?	false

-EndDateRange<DateTime>

Specifies the end time of the latest high level operation to delete

Required?	false
Default Value	DateTime.UtcNow
Accept Pipeline Input?	false

-IncludeIncomplete<SwitchParameter>

Specifies if incomplete high level operations should be deleted.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Examples

---------- **EXAMPLE 1** ----------

```
C:\PS> Remove-LogOperation  -UserName "DOMAIN\User"  -Password "UserPassword"
```
Remove all completed operation logs

---------- **EXAMPLE 2** ----------

```
C:\PS> Remove-LogOperation  -UserName "DOMAIN\User"  -Password "UserPassword" -IncludeIncomplete
```
Remove all operations

---------- **EXAMPLE 3** ----------

```
C:\PS> Remove-LogOperation -username "domain\userName" -password "password" -StartDateRange "2013-01-01 12:00:00"  -EndDateRange "2013-01-31 12:00:00"
```
Delete logs started on or after "2013-01-01 12:00:00" and completed on or before "2013-01-31 12:00:00"

---------- **EXAMPLE 4** ----------

```
C:\PS> $securePassword = ConvertTo-SecureString -String "UserPassword" -AsPlainText -Force
C:\PS> $credentials    = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList "DOMAIN\UserName", $securePassword
C:\PS> Remove-LogOperation -StartDateRange -DatabaseCredentials $credentials
```

Delete logs by supplying database user credentials via a credentials object.

Remove-LogServiceMetadata

Sep 10, 2014

Removes metadata from the given Service.

Syntax

```
Remove-LogServiceMetadata [-ServiceHostId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-LogServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-LogServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-LogServiceMetadata [-InputObject] <Service[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Service.

Related topics

Set-LogServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-LogService | % { Remove-LogServiceMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Service objects.

Remove-LogSiteMetadata

Sep 10, 2014

Removes metadata from the given Site.

Syntax

```
Remove-LogSiteMetadata -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]

Remove-LogSiteMetadata -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]

Remove-LogSiteMetadata -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]

Remove-LogSiteMetadata -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Site.

Related topics

Set-LogSiteMetadata

Parameters

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-LogSite | % { Remove-LogSiteMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Site objects.

Reset-LogDataStore

Sep 10, 2014

Refreshes the database string currently being used by the Log service.

Syntax

```
Reset-LogDataStore [-DataStore] <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Returns the string for the database connection currently being used by the ConfigurationLogging Service. Can only be called for secondary data stores.

There is no requirement for a database connection to be configured in order for this command to be used.

Related topics

Get-LogDataStore

Parameters

-DataStore<String>

Specifies the database connection logical name to be used by the ConfigurationLogging Service. Can be either be 'Site' or the logical name of the secondary data store. Specifying the site data store will display an error because this operation is not supported for site data stores.

Required?	true
Default Value	Site
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.ConfigurationLogging.Sdk.ServiceStatus

The status of the specified data store.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Reset-LogDataStore -DataStore Secondary
OK
```

Refresh the database connection string for the ConfigurationLogging Service.

Reset-LogServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the ConfigurationLogging Service.

Syntax

```
Reset-LogServiceGroupMembership [-ConfigServiceInstance] <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables you to reload ConfigurationLogging Service access permissions and configuration service locations. The Reset-LogServiceGroupMembership command must be run on at least one instance of the service type (Log) after installation and registration with the configuration service. Without this operation, the ConfigurationLogging services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-LogServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Parameters

-ConfigServiceInstance<ServiceInstance[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.ConfigurationLogging.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-LogServiceGroupMembership command.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-LogServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-LogServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Set-LogDBConnection

Sep 10, 2014

Configures a database connection for the ConfigurationLogging Service.

Syntax

```
Set-LogDBConnection [-DBConnection] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [[-DataStore] <String>] [<CommonParameters>]
```

Detailed Description

Configures a connection to a database in which the ConfigurationLogging Service can store its state. The service will attempt to connect and start using the database immediately after the connection is configured. The database connection string is updated to the specified value regardless of whether it is valid or not. Specifying an invalid connection string prevents a service from functioning until the error is corrected.

After a connection is configured, you cannot alter it without first clearing it (by setting the connection to $null).

You do not need to configure a database connection to use this command.

Related topics

Get-LogServiceStatus

Get-LogDBConnection

Test-LogDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the ConfigurationLogging Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

-DataStore<String>

Specifies the logical name of the data store for the ConfigurationLogging Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false
Default Value	Site
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-LogDBConnection command returns an object containing the status of the ConfigurationLogging Service together with extra diagnostics information.

DBUnconfigured

The ConfigurationLogging Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the ConfigurationLogging Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the ConfigurationLogging Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the ConfigurationLogging Service currently in use is incompatible with the version of the ConfigurationLogging Service schema on the database. Upgrade the ConfigurationLogging Service to a more recent version.

DBOlderVersionThanService

The version of the ConfigurationLogging Service schema on the database is incompatible with the version of the ConfigurationLogging Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The ConfigurationLogging Service is running and is connected to a database containing a valid schema.

Failed

The ConfigurationLogging Service has failed.

Unknown

The status of the ConfigurationLogging Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

DatabaseError

An error occurred in the service while attempting a database operation.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-LogDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Configures a database connection string for the ConfigurationLogging Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Set-LogDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Configures an invalid database connection string for the ConfigurationLogging Service.

Set-LogServiceMetadata

Sep 10, 2014

Adds or updates metadata on the given Service.

Syntax

Set-LogServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-LogServiceMetadata [-ServiceHostId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-LogServiceMetadata [-InputObject] <Service[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-LogServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Allows you to store additional custom data against given Service objects.

Related topics

Remove-LogServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Service specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-LogServiceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-LogServiceMetadata -ServiceHostId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Service with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-LogSite

Sep 10, 2014

Sets global configuration logging settings.

Syntax

Set-LogSite [-State <LoggingState>] [-Locale <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

This cmdlet sets the global configuration logging settings.

Related topics

Get-LogSite

Parameters

-State<LoggingState>

Sets the state of configuration logging. Values can be:

o Enabled - state changes will be logged. If logging is unavailable, the state change will still be permitted. o Disabled - state changes will not be logged.

o Mandatory - state change will be logged. If logging is unavailable, the state change will not be permitted.

When the state is set to Enabled or Mandatory, XenDesktop services will attempt to log operations (which perform configuration changes) before performing them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Locale<String>

Sets the language that logs should be recorded in. Values can be: 'en', 'ja', 'zh-CN', 'de', 'es' or 'fr'.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Returns the affected record. By default, this cmdlet does not generate any output.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.ConfigurationLogging.Sdk.Site

Current logging settings

Notes

Configuration logging will automatically transition to a 'NotSupported' state if the logging feature is not licensed. Set-LogSite will reject request to set logging to 'Enabled' or 'Mandatory' while the logging feature is not licensed.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Set-LogSite -Locale "zh-CN"
Set the logging language to Chinese. The logging state will be unchanged.

---------- EXAMPLE 2 ----------

C:\PS> Set-LogSite -State "Mandatory"
Set the logging state to mandatory. The logging locale will be unaffected. In this state, no configuration change will be allowed unless it is successfully logged.

---------- EXAMPLE 3 ----------

C:\PS> Set-LogSite -Locale "de" -State "Enabled"
Set the logging language to German and the state to Enabled.

Set-LogSiteMetadata

Sep 10, 2014

Adds or updates metadata on the given Site.

Syntax

```
Set-LogSiteMetadata -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-LogSiteMetadata -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-LogSiteMetadata -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-LogSiteMetadata -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability for additional custom data to be stored against given Site objects.

Related topics

Remove-LogSiteMetadata

Parameters

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Site specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-LogSiteMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-LogSiteMetadata -SiteDUMMY_IdProperty 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Site with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Start-LogHighLevelOperation

Sep 10, 2014

Logs the start of a high level operation.

Syntax

```
Start-LogHighLevelOperation -Text <String> -Source <String> [-StartTime <DateTime>] [-OperationType <OperationType>] [-TargetTypes <String[]>] [-Parameters <Hashtable>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Start-LogHighLevelOperation creates a log entry to record the start of a high level operation.

Start-LogHighLevelOperation can be called to log high level configuration changes which originate from customized configuration scripts. Start-LogHighLevelOperation should be called before the script invokes service SDK cmdlets which execute the configuration changes.

Start-LogHighLevelOperation returns a HighLevelOperation object which contains information about the started high level operation. The "Id" property of the returned HighLevelOperation uniquely identifies the started high level operation. This can be supplied into the "-LoggingId" parameter which is implemented in all service SDK cmdlets which execute loggable configuration changes.

High level operation logs are automatically created by the XenDesktop consoles when:

o Initiating an operation which performs configuration changes.

o Initiating an operation which performs an administration activity.

Configuration Change and Administrator Activity

A configuration change is an operation which alters the configuration of the XenDesktop site. Examples of a configuration changes include:

o Creating or editing a host.

o Creating or editing a catalog.

o Adding a user to a delivery group.

o Deleting a machine.

An administrator activity operation doesn't directly alter site configuration, but it could be an operation carried out by an administrator as part of site management or helpdesk support. Examples of administrator activities include:

o Shutdown/start/restart of a user desktop.

o Studio or Director sending a message to a user.

o Rebooting a user's desktop.

Once the change being logged has completed (whether successfully or not) the Stop-LogHighLevelOperation cmdlet should be called to log the completion of a started high level operation.

Related topics

Stop-LogHighLevelOperation

Get-LogHighLevelOperation

Parameters

-Text<String>

Specifies text to describe the high level operation.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Source<String>

Specifies the source of the high level operation.

Required?	true
Default Value	
Accept Pipeline Input?	false

-StartTime<DateTime>

Specifies the start time of the high level operation.

Required?	false
Default Value	DateTime.UtcNow
Accept Pipeline Input?	false

-OperationType<OperationType>

Specifies the type of operation being logged. Values can be:

o AdminActivity - If the operation being logged performs an administration activity.

o ConfigurationChange - If the operation being logged performs a configuration change.

Required?	false
Default Value	ConfigurationChange
Accept Pipeline Input?	false

-TargetTypes<String[]>

Specifies the names of the object types that will be affected by the operation being logged.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Parameters<Hashtable>

Specifies the names and values of parameters that are supplied to the operation being logged.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.ConfigurationLogging.Sdk.HighLevelOperation

The newly logged high level operation start.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $succeeded = $false #indicates if high level operation succeeded.
C:\PS> # Log high level operation start.
C:\PS> $highLevelOp = Start-LogHighLevelOperation -Text "Create catalog" -Source "My Custom Script"
C:\PS>
C:\PS> try
C:\PS> {
C:\PS>   # Create catalog object
C:\PS>   $catalog = New-BrokerCatalog -Name "MyCatalog" -ProvisioningType Manual -AllocationType Permanent -MinimumFunctionalLevel 'LMAX' -LoggingId $highLevelC
C:\PS>
```

```
C:\PS>   # Add a machine to the catalog
C:\PS>   $machine = New-BrokerMachine -CatalogUid $catalog.Uid -MachineName "DOMAIN\Machine" -LoggingId $highLevelOp.Id
C:\PS>   $succeeded = $true
C:\PS> }
C:\PS> catch{ "Error encountered" }
C:\PS>
C:\PS> finally{
C:\PS>   # Log high level operation stop, and indicate its success
C:\PS>   Stop-LogHighLevelOperation -HighLevelOperationId $highLevelOp.Id -IsSuccessful $succeeded
C:\PS> }
```

Creates an unmanaged catalog and assigns a machine to it, within the scope of a high level operation start and stop. The identifier of the high level operation is passed into the "-LoggingId" parameter of the service SDK cmdlets. The execution of the cmdlets in the services will create the low level operation logs for the supplied high level operation.

Stop-LogHighLevelOperation

Sep 10, 2014

Logs the completion of a previously started high level operation.

Syntax

```
Stop-LogHighLevelOperation -HighLevelOperationId <String> -IsSuccessful <Boolean> [-EndTime <DateTime>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Stop-LogHighLevelOperation logs the completion of a started high level operation.

Related topics

Start-LogHighLevelOperation

Get-LogHighLevelOperation

Parameters

-HighLevelOperationId<String>

Specifies the identifier of the high level operation being completed.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IsSuccessful<Boolean>

Specifies if the started high level operation completed sucessfully.

Required?	true
Default Value	
Accept Pipeline Input?	false

-EndTime<DateTime>

Specifies the end time of the high level operation being completed.

Required?	false
Default Value	DateTime.UtcNow.
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $succeeded = $false #indicates if high level operation succeeded.
C:\PS> # Log high level operation start.
C:\PS> $highLevelOp = Start-LogHighLevelOperation -Text "Create unmanaged catalog" -Source "My Custom Script"
C:\PS>
C:\PS> try
C:\PS> {
C:\PS>   # Create catalog object
C:\PS>   $catalog = New-BrokerCatalog -Name "MyCatalog" -ProvisioningType Manual -AllocationType Permanent -MinimumFunctionalLevel 'LMAX' -LoggingId $highLevelC
```

```
C:\PS>
C:\PS>   # Add a machine to the catalog
C:\PS>   $machine = New-BrokerMachine -CatalogUid $catalog.Uid -MachineName "DOMAIN\Machine" -LoggingId $highLevelOp.Id
C:\PS>   $succeeded = $true
C:\PS> }
C:\PS> catch{ "Error encountered" }
C:\PS>
C:\PS> finally{
C:\PS>   # Log high level operation stop, and indicate its success
C:\PS>   Stop-LogHighLevelOperation -HighLevelOperationId $highLevelOp.Id -IsSuccessful $succeeded
C:\PS> }
```

Creates an unmanaged catalog and assigns a machine to it, within the scope of a high level operation start and stop. The identifier of the high level operation is passed into the "-LoggingId" parameter of the service SDK cmdlets. The execution of the cmdlets in the services will create the low level operation logs for the supplied high level operation.

Test-LogDBConnection

Sep 10, 2014

Tests a database connection for the ConfigurationLogging Service.

Syntax

```
Test-LogDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [[-DataStore] <String>]
[<CommonParameters>]
```

Detailed Description

Tests a connection to the database in which the ConfigurationLogging Service can store its state. The service will attempt to connect to the database without affecting the current connection to the database.

You do not have to clear the connection to use this command.

Related topics

Get-LogServiceStatus

Get-LogDBConnection

Set-LogDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the ConfigurationLogging Service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

-DataStore<String>

Specifies the logical name of the data store for the ConfigurationLogging Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false
Default Value	Site
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-LogDBConnection command returns an object containing the status of the ConfigurationLogging Service if the connection string of the specified data store were to be set to the string being tested, together with extra diagnostics information for the specified connection string.

DBRejectedConnection

The database rejected the logon attempt from the ConfigurationLogging Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the ConfigurationLogging Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the ConfigurationLogging Service currently in use is incompatible with the version of the ConfigurationLogging Service schema on the database. Upgrade the ConfigurationLogging Service to a more recent version.

DBOlderVersionThanService

The version of the ConfigurationLogging Service schema on the database is incompatible with the version of the ConfigurationLogging Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Set-LogDBConnection command would succeed if it were executed with the supplied connection string.

Failed

The ConfigurationLogging Service has failed.

Unknown

The status of the ConfigurationLogging Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseError

An error occurred in the service while attempting a database operation.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Test-LogDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Tests a database connection string for the ConfigurationLogging Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Test-LogDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Tests an invalid database connection string for the ConfigurationLogging Service.

Citrix.DelegatedAdmin.Admin.V1

Sep 10, 2014

Overview

Name	Description
AdminDelegatedAdminSnapin	The Delegated Administration Service PowerShell snap-in provides
Admin Filtering	Describes the common filtering options for XenDesktop cmdlets.

Cmdlets

Name	Description
Add-AdminPermission	Add permissions to the set of permissions of a role.
Add-AdminRight	Grants a given right to the specified administrator.
Get-AdminAdministrator	Gets administrators configured for this site.
Get-AdminDBConnection	Gets the database string for the specified data store used by the DelegatedAdmin Service.
Get-AdminDBSchema	Gets a script that creates the DelegatedAdmin Service database schema for the specified data store.
Get-AdminDBVersionChangeScript	Gets a script that updates the DelegatedAdmin Service database schema.
Get-AdminEffectiveAdministrator	Retrieve the effective administrator objects for a user.
Get-AdminEffectiveRight	Gets the set of Right objects associated with the current user.
Get-AdminInstalledDBVersion	Gets a list of all available database schema versions for the DelegatedAdmin Service.
Get-AdminPermission	Gets permissions configured for the site.
Get-AdminPermissionGroup	Gets permission groups configured for the site.
Get-AdminRevision	Gets the current revision of the delegated administration configuration data.

Name	Description
Get-AdminRole	Gets roles configured for this site.
Get-AdminRoleConfiguration	Gets role configurations for this site.
Get-AdminScope	Gets scopes configured for this site.
Get-AdminService	Gets the service record entries for the DelegatedAdmin Service.
Get-AdminServiceAddedCapability	Gets any added capabilities for the DelegatedAdmin Service on the controller.
Get-AdminServiceInstance	Gets the service instance entries for the DelegatedAdmin Service.
Get-AdminServiceStatus	Gets the current status of the DelegatedAdmin Service on the controller.
Import-AdminRoleConfiguration	Imports role configuration data into the Delegated Administration Service.
New-AdminAdministrator	Adds a new administrator to the site.
New-AdminRole	Adds a new custom role to the site.
New-AdminScope	Adds a new scope to the site.
Remove-AdminAdministrator	Removes administrators from the site.
Remove-AdminAdministratorMetadata	Removes metadata from the given Administrator.
Remove-AdminPermission	Remove permissions from the set of permissions of a role.
Remove-AdminRight	Removes rights from an administrator.
Remove-AdminRole	Removes a role from the site.
Remove-AdminRoleMetadata	Removes metadata from the given Role.
Remove-AdminScope	Removes a scope from the site.
Remove-AdminScopeMetadata	Removes metadata from the given Scope.

Name	Description
Remove-AdminServiceMetadata	Removes metadata from the given Service.
Rename-AdminRole	Rename a role
Rename-AdminScope	Rename a scope
Reset-AdminServiceGroupMembership	Reloads the access permissions and configuration service locations for the DelegatedAdmin Service.
Set-AdminAdministrator	Sets the properties of an administrator.
Set-AdminAdministratorMetadata	Adds or updates metadata on the given Administrator.
Set-AdminDBConnection	Configures a database connection for the DelegatedAdmin Service.
Set-AdminRole	Set the properties of a role.
Set-AdminRoleMetadata	Adds or updates metadata on the given Role.
Set-AdminScope	Set the properties of a scope.
Set-AdminScopeMetadata	Adds or updates metadata on the given Scope.
Set-AdminServiceMetadata	Adds or updates metadata on the given Service.
Test-AdminAccess	Retrieves the scopes where the specified operation is permitted.
Test-AdminDBConnection	Tests a database connection for the DelegatedAdmin Service.

about_AdminDelegatedAdminSnapin

Sep 10, 2014

TOPIC

about_AdminDelegatedAdminSnapin

SHORT DESCRIPTION

The Delegated Administration Service PowerShell snap-in provides administrative functions for the Delegated Administration Service.

COMMAND PREFIX

All commands in this snap-in are prefixed with 'Admin'.

LONG DESCRIPTION

The Delegated Administration Service PowerShell snap-in enables both local and remote administration of the Delegated Administration Service.

The Delegated Administration Service (or DAS for short) stores information about Citrix administrators and the rights they have. Services in the XenDesktop deployment use the DAS to determine whether a particular user has the privilege to perform an operation or not.

The snap-in provides storage and configuration of these entities:

Administrators

> Each administrator object represents an individual person or a group of people identified by their Active Directory account. Administrators can be enabled and disabled.
>
> The effective rights that a user has is the union of any rights that they have by looking at their Active Directory group membership. Disabled administrator entries are ignored for this calculation.
>
> Once a site is setup, there must always be a full administrator and the Delegated Administration snap-in rejects requests to remove or disable the last full administrator.

Roles

> A role represents a job function. That is, anyone with a given role is expected to be able to use or perform the tasks, wizards, and actions associated with that role. Administrators may have multiple roles for a particular site.

Some roles are built-in, and some editions of the product allow custom roles to be created with different combinations of permissions.

Scopes

Scopes represent a collection of objects, and are used to group objects for administrative purposes in a way that is relevant to the organisation. They can be used to represent both hierarchical and non-hierarchical relationships.

Objects can exist in multiple scopes at once. You may find it easier to think of scopes as labels, or a non-exclusive grouping such as a play-list.

All objects are implicitly in the built-in 'All' scope.

Some objects are not scoped, and access to them is through either the 'All' scope or indirectly through a scoped object. For example sessions are not directly scoped but can be accessed using the scope of the desktop group.

The DAS stores information about scopes, but the mapping between scopes and objects is stored and updated using the PowerShell snap-ins of each corresponding service. For example, Delivery Group scopes are managed using the Broker PowerShell snap-in.

Rights

Rights determine what an administrator can do and where they can do it. They are expressed as a number of <role, scope> pairs associated with each administrator.

To gain access to any particular object, a person must match an administrator object that has an appropriate right that allows the required operation in a scope that the object is a member of.

Permissions

Each task, wizard or action in the Citrix Studio or Director consoles represents a unit of functionality that an administrator can perform. Permissions are expressed at a high level and generally correspond directly to the labels in the consoles. For example: "Edit catalog", or "Create delivery group".

Permission groups:

Permissions are grouped into related functionality when displayed by the console.

Operations

Operations are the indivisible unit of functionality that each XenDesktop service can perform, and usually correspond to individual cmdlets. Internally, each permission requires a number of operations to be performed, possibly by different services.

about_Admin_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```


retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

A120901
B220000
...

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

Add-AdminPermission

Sep 10, 2014

Add permissions to the set of permissions of a role.

Syntax

```
Add-AdminPermission [-InputObject] <Permission[]> -Role <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-AdminPermission [-Permission] <String[]> -Role <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Add extra permissions to the set of permissions that a role maps to.

Any administrator with a right including that role immediately gains the ability to use the operations of the new permissions.

Duplicate permissions do not produce an error, and permissions are skipped if the role already contains the permission (without error).

You cannot modify the permissions of built-in roles.

Related topics

Remove-AdminPermission

Get-AdminPermission

Get-AdminRole

Get-AdminPermissionGroup

Test-AdminAccess

Parameters

-InputObject<Permission[]>

Specifies the permissions to add.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Permission<String[]>

Specifies the list of permissions to add (by identifier).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Role<String>

Role name or identifier of the role to update.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Permission You can pipe a list of permissions to be added into this command.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Add-AdminPermission -Role MyRole -Permission Global_Read,Logging_Read
```

Add a couple of specific permissions to the 'MyRole' role.

---------- EXAMPLE 2 ----------

```
C:\PS> $list = Get-AdminRole "Delivery Administrator" | Select -Expand Permissions
C:\PS> Add-AdminPermission -Role MyRole -Permission $list
```

Add all of the permissions of the Delivery Administrator role to MyRole.

Add-AdminRight

Sep 10, 2014

Grants a given right to the specified administrator.

Syntax

```
Add-AdminRight -Scope <String> -Role <String> -Administrator <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-AdminRight -Role <String> -Administrator <String> [-All] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-AdminRight [-InputObject] <Right[]> -Administrator <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use the Add-AdminRight cmdlet to add rights (role and scope pairs) to an administrator.

For convenience, you can use the -All parameter to specify the 'All' scope.

Use the Get-AdminAdministrator cmdlet to determine what rights an administrator has.

Related topics

Get-AdminAdministrator

Get-AdminEffectiveRight

Remove-AdminRight

Parameters

-InputObject<Right[]>

Specifies the rights to add from Right objects.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Scope<String>

Specifies the scope name or scope identifier.

Required?	true

Default Value	
Accept Pipeline Input?	false

-Role<String>

Specifies the role name or role identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Administrator<String>

Specifies the name or SID of the administrator.

Required?	true
Default Value	
Accept Pipeline Input?	false

-All<SwitchParameter>

Specifies the 'All' scope. This parameter avoids localization issues or having to type the identifier of the 'All' scope.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Right You can pipe the rights to be added into this command.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Add-AdminRight -Role 'Help Desk Administrator' -Scope London -Administrator DOMAIN\Admin1
```

Assigns the 'Help Desk Administrator' role and 'London' scope to the 'Admin1' administrator.

---------- EXAMPLE 2 ----------

```
C:\PS> Add-AdminRight -Role 'Full Administrator' -All -Administrator DOMAIN\Admin1
```

Assigns the 'Full Administrator' role and 'All' scope to the 'Admin1' administrator.

---------- EXAMPLE 3 ----------

```
C:\PS> $admin = Get-AdminAdministrator -Name DOMAIN\ExistingAdmin
C:\PS> Add-AdminRight -InputObject $admin.Rights -Administrator DOMAIN\NewAdmin
```

Copies the administrator rights from 'ExistingAdmin' to 'NewAdmin'.

Get-AdminAdministrator

Sep 10, 2014

Gets administrators configured for this site.

Syntax

```
Get-AdminAdministrator [[-Name] <String>] [-Sid <String>] [-Enabled <Boolean>] [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Retrieves administrators matching the specified criteria. If no parameters are specified this cmdlet enumerates all administrators.

See about_Admin_Filtering for information about advanced filtering options.

Related topics

New-AdminAdministrator

Set-AdminAdministrator

Remove-AdminAdministrator

Set-AdminAdministratorMetadata

Remove-AdminAdministratorMetadata

Parameters

-Name<String>

Gets administrators with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Sid<String>

Gets administrators with the specified SID (security identifier).

Required?	false
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Gets administrators with the specified value of Enabled.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Admin_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Admin_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.Administrator

Get-AdminAdministrator returns an object for each matching administrator.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-AdminAdministrator -Name DOMAIN\TestUser
```

Finds the administrator object (if one exists) for user "DOMAIN\TestUser".

---------- EXAMPLE 2 ----------

```
C:\PS> Get-AdminAdministrator -Enabled $false
```

Finds all disabled administrator objects.

Get-AdminDBConnection

Sep 10, 2014

Gets the database string for the specified data store used by the DelegatedAdmin Service.

Syntax

```
Get-AdminDBConnection [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the database connection string for the specified data store.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

Related topics

Get-AdminServiceStatus

Set-AdminDBConnection

Test-AdminDBConnection

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

system.string

The database connection string configured for the DelegatedAdmin Service.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the DelegatedAdmin Service has not been specified.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminDBConnection

Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True
```

Get the database connection string for the DelegatedAdmin Service.

Get-AdminDBSchema

Sep 10, 2014

Gets a script that creates the DelegatedAdmin Service database schema for the specified data store.

Syntax

```
Get-AdminDBSchema [-DatabaseName <String>] [-ServiceGroupName <String>] [-ScriptType <ScriptTypes>] [-LocalDatabase] [-Sid <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets SQL scripts that can be used to create a new DelegatedAdmin Service database schema, add a new DelegatedAdmin Service to an existing site, remove a DelegatedAdmin Service from a site, or create a database server logon for a DelegatedAdmin Service. If no Sid parameter is provided, the scripts obtained relate to the currently selected DelegatedAdmin Service instance, otherwise the scripts relate to DelegatedAdmin Service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied. The current service instance is that on the local machine, or that explicitly specified by the last usage of the -AdminAddress parameter to a DelegatedAdmin SDK cmdlet. The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured. The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SMDCMD mode'. The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to DelegatedAdmin Service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to DelegatedAdmin Service roles

If ScriptType is Evict, the returned script contains:

o Removal of DelegatedAdmin Service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database. You do not need to configure a database before using this command.

Related topics

Set-AdminDBConnection

Parameters

-DatabaseName<String>

Specifies the name of the database for which the schema will be generated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the DelegatedAdmin services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<ScriptTypes>

Specifies the type of database script returned. Available script types are:

Database

Returns a full database script that can be used to create a database schema for the DelegatedAdmin Service in a database instance that does not already contain a schema for this service. The DatabaseName and ServiceGroupName parameters must be specified to create a script of this type.

Instance

Returns a permissions script that can be used to add further DelegatedAdmin services to an existing database instance that already contains the full DelegatedAdmin service schema, associating the services to the Service Group. The Sid parameter can optionally be specified to create a script of this type.

Login

Returns a database logon script that can be used to add the required logon accounts to an existing database instance that contains the DelegatedAdmin Service schema. This is used primarily when creating a mirrored database environment. The DatabaseName parameter must be specified to create a script of this type.

Evict

Returns a script that can be used to remove the specified DelegatedAdmin Service from the database entirely. The DatabaseName and Sid parameters must be specified to create a script of this type.

Required?	false
Default Value	Database
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for DelegatedAdmin services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Sid<String>

Specifies the SID of the controller on which the DelegatedAdmin Service instance to remove from the database is running.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.string

A string containing the required SQL script for application to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminDBSchema -DatabaseName MyDB -ServiceGroupName  MyServiceGroup > c:\AdminSchema.sql
```

Get the full database schema for site data store of the DelegatedAdmin Service and copy it to a file called 'c:\AdminSchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a DelegatedAdmin Service site schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-AdminDBSchema -DatabaseName MyDB -scriptType Login > c:\DelegatedAdminLogins.sql
```

Get the logon scripts for the DelegatedAdmin Service.

Get-AdminDBVersionChangeScript

Sep 10, 2014

Gets a script that updates the DelegatedAdmin Service database schema.

Syntax

```
Get-AdminDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a database script that can be used to upgrade or downgrade the site or secondary schema for the DelegatedAdmin Service from the current schema version to a different version.

Related topics

Get-AdminInstalledDBVersion

Parameters

-DatabaseName<String>

Specifies the name of the database instance to which the update applies.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

Specifies the version of the database you want to update to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

A PSObject containing the required SQL script for application to a database.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any DelegatedAdmin services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-AdminServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the DelegatedAdmin Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS> $update = Get-AdminDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-AdminEffectiveAdministrator

Sep 10, 2014

Retrieve the effective administrator objects for a user.

Syntax

```
Get-AdminEffectiveAdministrator [-Name] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This command determines what groups the specified user belongs to and retrieves the matching administrator records. It includes the set of rights that would be granted to the user if he or she used the system.

As this command uses Active Directory to determine what groups the user has, the caller must have the ability to read this information from Active Directory.

Only enabled administrator records are returned.

Related topics

Get-AdminAdministrator

Parameters

-Name<String>

User name or SID of user to query

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

string User name or SID of user to query

Return Values

Citrix.DelegatedAdmin.Sdk.Administrator

Administrator records matching the specified user

Examples

-------------------------- EXAMPLE 1 --------------------------

C:\PS> Get-AdminEffectiveAdministrator MYDOMAIN\testuser
Retrieve the administrator records matching user 'testuser'.

Get-AdminEffectiveRight

Sep 10, 2014

Gets the set of Right objects associated with the current user.

Syntax

```
Get-AdminEffectiveRight [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Get-AdminEffectiveRight cmdlet returns the effective rights of the current user. This is the union of all rights of the enabled administrators that the current user matches, taking into account Active Directory group membership.

Related topics

Get-AdminAdministrator

Add-AdminRight

Remove-AdminRight

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.Right

The Rights associated with the current user

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-AdminEffectiveRight
```

Return the effective rights for the current user.

Get-AdminInstalledDBVersion

Sep 10, 2014

Gets a list of all available database schema versions for the DelegatedAdmin Service.

Syntax

```
Get-AdminInstalledDBVersion [-Upgrade] [-Downgrade] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the current version of the DelegatedAdmin Service database schema, if no flags are set, otherwise returns versions for which upgrade or downgrade scripts are available and have been stored in the database.

Related topics

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Version

The Get-AdminInstalledDbVersion command returns objects containing the new definition of the DelegatedAdmin Service database schema version.

Major <Integer>

Minor <Integer>

Build <Integer>

Revision <Integer>

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the DelegatedAdmin Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminInstalledDBVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      6      0      0
```

Get the currently installed version of the DelegatedAdmin Service database schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-AdminInstalledDBVersion -Upgrade

Major  Minor  Build  Revision
-----  -----  -----  --------
6      0      0      0
```

Get the versions of the DelegatedAdmin Service database schema for which upgrade scripts are supplied.

Get-AdminPermission

Sep 10, 2014

Gets permissions configured for the site.

Syntax

```
Get-AdminPermission [[-Name] <String>] [-Id <String>] [-Description <String>] [-GroupId <String>] [-GroupName <String>] [-Metadata <String>] [-Operation <String>] [-ReadOnly <Boolean>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Retrieves permission matching the specified criteria. If no parameters are specified this cmdlet enumerates all permissions.

Permissions are configured using the Import-AdminRoleConfiguration command, and are used to represent collections of operations that are needed to perform a particular task. These permissions are presented in Citrix Studio when configuring roles.

Permissions can also have metadata associated with them.

See about_Admin_Filtering for information about advanced filtering options.

Related topics

Add-AdminPermission

Remove-AdminPermission

Get-AdminRole

Get-AdminPermissionGroup

Test-AdminAccess

Parameters

-Name<String>

Gets permissions with the specified name (localized)

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Id<String>

Gets permissions with the specified identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Gets permissions with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-GroupId<String>

Gets permissions that are a member of the specified permission group (by group id).

Required?	false
Default Value	
Accept Pipeline Input?	false

-GroupName<String>

Gets permissions that are a member of the specified permission group (by group name).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Operation<String>

Gets permissions that contain a specific operation.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReadOnly<Boolean>

Gets permissions with the specified value for the ReadOnly flag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Admin_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0

Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Admin_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.Permission

Get-AdminPermission returns an object for each matching permission.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-AdminPermission -Name *Edit*
```
Finds all permissions with 'Edit' in their names.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-AdminPermission -Operation "Broker:SetCatalog"
C:\PS> Get-AdminPermission -Filter { Operations -contains "Broker:SetCatalog" -or Operations -contains "Broker:NewCatalog" }
```
Finds permissions that contain specific operations, with the -Filter form needed to match multiple values.

Get-AdminPermissionGroup

Sep 10, 2014

Gets permission groups configured for the site.

Syntax

```
Get-AdminPermissionGroup [[-Name] <String>] [-Id <String>] [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Retrieves permission groups matching the specified criteria. If no parameters are specified this cmdlet enumerates all permission groups.

Permission groups are configured using the Import-AdminRoleConfiguration command, and are primarily used to store the localized name for a group of permissions. Permission groups can also have metadata associated with them.

See about_Admin_Filtering for information about advanced filtering options.

Related topics

Import-AdminRoleConfiguration

Get-AdminPermission

Parameters

-Name<String>

Gets permission groups matching the given name. This is the localized name of the group.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Id<String>

Gets permission groups with the given identifier. This is the non-localized identifier used to associate permissions with permission groups.

Required?	false
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Admin_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false

Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Admin_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.PermissionGroup

Get-AdminPermissionGroup returns an object for each matching permission group.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-AdminPermissionGroup -Name *s
```

Finds all permission groups that end with the letter 's'.

---------- EXAMPLE 2 ----------

```
C:\PS> $list = @("Hosts","Other")
C:\PS> Get-AdminPermissionGroup -Filter { Id -in $list } -SortBy Name
```

Retrieve two specific permission group objects with the matching identifiers.

Get-AdminRevision

Sep 10, 2014

Gets the current revision of the delegated administration configuration data.

Syntax

```
Get-AdminRevision [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Delegated Administration Service maintains a revision number that is incremented whenever its configuration is changed. This command retrieves the current revision number.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

System.Int32

The configuration revision number

Notes

If Int32.MaxValue is reached the value of the revision number will wrap around to Int32.MinValue.

In some cases the value may be incremented by more than one.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-AdminRevision
```

Retrieve the current revision number.

Get-AdminRole

Sep 10, 2014

Gets roles configured for this site.

Syntax

Get-AdminRole [[-Name] <String>] [-Id <Guid>] [-BuiltIn <Boolean>] [-Description <String>] [-Metadata <String>] [-Permission <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieves roles matching the specified criteria. If no parameters are specified, this cmdlet enumerates all roles.

See about_Admin_Filtering for information about advanced filtering options.

Related topics

New-AdminRole

Set-AdminRole

Rename-AdminRole

Remove-AdminRole

Set-AdminRoleMetadata

Remove-AdminRoleMetadata

Parameters

-Name<String>

Gets roles with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Id<Guid>

Gets the role with the specified identifier.

Required?	false

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-BuiltIn<Boolean>

Gets roles with the specified value of the BuiltIn flag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets roles with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Permission<String>

Gets roles that contain a specific permission.

Required?	false

Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Admin_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Admin_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.Role

Get-AdminRole returns an object for each matching role.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-AdminRole -Id 20852cdf-f527-4953-ba6e-e7545217122d
```

Gets the details of the role with the specific id.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-AdminRole -BuiltIn $false
```

List all custom roles.

Get-AdminRoleConfiguration

Sep 10, 2014

Gets role configurations for this site.

Syntax

```
Get-AdminRoleConfiguration [[-Name] <String>] [-Id <Guid>] [-Locale <String>] [-Priority <Int32>] [-Version <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Retrieves role configurations matching the specified criteria. If no parameters are specified, this cmdlet enumerates and returns all role configurations.

Role configurations are part of the product configuration and define what permissions, permission groups, and built-in roles the product has. This cmdlet also provides the mapping of permissions to operations.

Related topics

Import-AdminRoleConfiguration

Parameters

-Name<String>

Gets role configurations matching the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Id<Guid>

Gets role configurations with the specified id.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Locale<String>

Gets role configurations with the specified locale. Role configurations usually have a consistent locale.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Priority<Int32>

Gets role configurations with the specified priority.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Version<String>

Gets role configurations with the matching version number.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Admin_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Admin_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.RoleConfiguration

Get-AdminRoleConfiguration returns an object for each matching role configuration.

Notes

This command is supplied for infrastructure purposes only and is not intended for public use.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-AdminRoleConfiguration -Name Director
```

Retrieve the role configuration for the Citrix Director component.

Get-AdminScope

Sep 10, 2014

Gets scopes configured for this site.

Syntax

Get-AdminScope [[-Name] <String>] [-Id <Guid>] [-BuiltIn <Boolean>] [-Description <String>] [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieves scopes matching the specified criteria. If no parameters are specified this cmdlet enumerates all scopes.

There is one special built-in scope, the 'All' scope.

To determine what objects are currently in a scope, use the Get-<Prefix>ScopedObject from each of the relevant PowerShell snap-ins.

See about_Admin_Filtering for information about advanced filtering options.

Related topics

New-AdminScope

Set-AdminScope

Rename-AdminScope

Remove-AdminScope

Set-AdminScopeMetadata

Remove-AdminScopeMetadata

Parameters

-Name<String>

Gets scopes with the specified name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-Id<Guid>

Gets the scope with the specified identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-BuiltIn<Boolean>

Gets scopes with the specified value of the BuiltIn flag.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Description<String>

Gets scopes with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Admin_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0

Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Admin_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.Scope

Get-AdminScope returns an object for each matching scope.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-AdminScope -Name *Sales*
```

List all scopes that contain the word 'Sales'.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-AdminScope -Id 21862daf-e529-4553-ba6e-f7543217111e
```

Gets the details of the scope with the specific id.

Get-AdminService

Sep 10, 2014

Gets the service record entries for the DelegatedAdmin Service.

Syntax

```
Get-AdminService [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns instances of the DelegatedAdmin Service that the service publishes. The service records contain account security identifier information that can be used to remove each service from the database.

A database connection for the service is required to use this command.

Related topics

Parameters

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Admin_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Admin_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.DelegatedAdmin.Sdk.Service

The Get-AdminServiceInstance command returns an object containing the following properties.

Uid <Integer>

Specifies the unique identifier for the service in the group. The unique identifier is an index number.

ServiceHostId <Guid>

Specifies the unique identifier for the service instance.

DNSName <String>

Specifies the domain name of the host on which the service runs.

MachineName <String>

Specifies the short name of the host on which the service runs.

CurrentState <Citrix.Fma.Sdk.ServiceCore.ServiceState>

Specifies whether the service is running, started but inactive, stopped, or failed.

LastStartTime <DateTime>

Specifies the date and time at which the service was last restarted.

LastActivityTime <DateTime>

Specifies the date and time at which the service was last stopped or restarted.

OSType

Specifies the operating system installed on the host on which the service runs.

OSVersion

Specifies the version of the operating system installed on the host on which the service runs.

ServiceVersion

Specifies the version number of the service instance. The version number is a string that reflects the full build version of the service.

DatabaseUserName <string>

Specifies for the service instance the Active Directory account name with permissions to access the database. This will be either the machine account or, if the database is running on a controller, the NetworkService account.

Sid <string>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

ActiveSiteServices <string[]>

Specifies the names of active site services currently running in the service. Site services are components that perform long-running background processing in some services. This field is empty for services that do not contain site services.

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminService

Uid             : 1
ServiceHostId     : aef6f464-f1ee-4042-a523-66982e0cecd0
DNSName           : MyServer.company.com
MachineName       : MYSERVER
CurrentState      : On
LastStartTime     : 04/04/2011 15:25:38
LastActivityTime  : 04/04/2011 15:33:39
OSType            : Win32NT
OSVersion         : 6.1.7600.0
ServiceVersion    : 5.1.0.0
DatabaseUserName  : NT AUTHORITY\NETWORK SERVICE
SID               : S-1-5-21-2316621082-1546847349-2782505528-1165
ActiveSiteServices : {MySiteService1, MySiteService2...}
```

Get all the instances of the DelegatedAdmin Service running in the current service group.

Get-AdminServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the DelegatedAdmin Service on the controller.

Syntax

```
Get-AdminServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the DelegatedAdmin Service on the controller to be detected.

You do not need to configure a database connection before using this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminServiceAddedCapability
```

Get the added capabilities of the DelegatedAdmin Service.

Get-AdminServiceInstance

Sep 10, 2014

Gets the service instance entries for the DelegatedAdmin Service.

Syntax

```
Get-AdminServiceInstance [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns service interfaces published by the instance of the DelegatedAdmin Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.DelegatedAdmin.Sdk.ServiceInstance

The Get-AdminServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a

central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

Specifies the service instance type. For this service, the service instance type is always Admin.

Address

Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

SDK - for PowerShell operations

InterService - for operations between different services

Peer - for communications between services of the same type

Metadata <Citrix.DelegatedAdmin.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminServiceInstance

Address          : http://MyServer.com:80/Citrix/DelegatedAdminContract
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         :
MetadataMap      :
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName  : MyServiceGroup
ServiceGroupUid   : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType      : Admin
Version          : 1

Address          : http://MyServer.com:80/Citrix/DelegatedAdminContract/IServiceApi
Binding          : wcf_HTTP_kerb
InterfaceType    : InterService
Metadata         :
MetadataMap      :
```



```
ServiceAccount     : ENG\MyAccount
ServiceAccountSid  : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName   : MyServiceGroup
ServiceGroupUid    : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType        : Admin
Version            : 1
```

Get all instances of the DelegatedAdmin Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-AdminServiceStatus

Sep 10, 2014

Gets the current status of the DelegatedAdmin Service on the controller.

Syntax

```
Get-AdminServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the DelegatedAdmin Service on the controller to be monitored. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured.

Related topics

Set-AdminDBConnection

Test-AdminDBConnection

Get-AdminDBConnection

Get-AdminDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-AdminServiceStatus command returns an object containing the status of the DelegatedAdmin Service together with extra diagnostics information.

DBUnconfigured

The DelegatedAdmin Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the DelegatedAdmin Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the DelegatedAdmin Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the DelegatedAdmin Service currently in use is incompatible with the version of the DelegatedAdmin Service schema on the database. Upgrade the DelegatedAdmin Service to a more recent version.

DBOlderVersionThanService

The version of the DelegatedAdmin Service schema on the database is incompatible with the version of the DelegatedAdmin Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The DelegatedAdmin Service is running and is connected to a database containing a valid schema.

Failed

The DelegatedAdmin Service has failed.

Unknown

(0) The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminServiceStatus
```

DBUnconfigured
Get the current status of the DelegatedAdmin Service.

Import-AdminRoleConfiguration

Sep 10, 2014

Imports role configuration data into the Delegated Administration Service.

Syntax

```
Import-AdminRoleConfiguration [-Path] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Import-AdminRoleConfiguration -Content <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This command is intended for use by Citrix Studio to import definitions, roles, permissions, and their mappings to operations.

The supplied configuration requires a digital signature; this is used to validate the integrity of the configuration.

Related topics

Get-AdminRoleConfiguration

Parameters

-Path<String>

The path to the file containing the role configuration data.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Content<String>

The content of the role configuration data.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Force<SwitchParameter>

Allows older versions of role configuration to replace newer versions.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

None

Notes

This command is supplied for infrastructure purposes only and is not intended for public use.

Examples

---------- EXAMPLE 1 ----------

C:\PS> Import-AdminRoleConfiguration -Path 'C:\MyAdminConfig.xml'
Imports the contents of 'C:\MyAdminConfig.xml' to the Delegated Administration Service.

New-AdminAdministrator

Sep 10, 2014

Adds a new administrator to the site.

Syntax

```
New-AdminAdministrator [-Name] <String> [-Enabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-AdminAdministrator -Sid <String> [-Enabled <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

New-AdminAdministrator creates a new administrator object in the site. Once a new administrator has been created you can assign rights (role and scope pairs) to the administrator.

Administrator objects are used to determine what rights, and therefore what permissions a particular Active Directory user has through the various SDKs and consoles of the site.

When the Enabled flag of an administrator is set to false, any rights of the administrator are ignored by the system when performing permission checks.

Related topics

Get-AdminAdministrator

Set-AdminAdministrator

Remove-AdminAdministrator

Set-AdminAdministratorMetadata

Remove-AdminAdministratorMetadata

Parameters

-Name<String>

Specifies the user or group name in Active Directory that this administrator corresponds to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Sid<String>

Specifies the SID (security identifier) of the user in Active Directory that this administrator corresponds to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Specifies whether the new administrator starts off enabled or not.

Required?	false
Default Value	True
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.Administrator

The newly created administrator.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-AdminAdministrator -Name DOMAIN\TestUser
```

Creates a new administrator object for user "DOMAIN\TestUser". It defaults to enabled.

---------- EXAMPLE 2 ----------

```
C:\PS> New-AdminAdministrator -Sid S-1-2-34-1234567890-1234567890-1234567890-123
```

Creates a new administrator object for user with SID "S-1-2-34-1234567890-1234567890-1234567890-123". It defaults to enabled.

New-AdminRole

Sep 10, 2014

Adds a new custom role to the site.

Syntax

```
New-AdminRole [-Name] <String> [-Description <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

New-AdminRole adds a new custom role object to the site. Once a new role has been created, you can add permissions to the role which define what operations the role conveys.

Roles represent a job function, such as 'help desk administrator', and contain a list of permissions that are required to perform that job function.

To assign a role to an administrator, you combine it with a scope which indicates what objects the role can operate on. This pair (also known as a 'right') can then be assigned to an administrator. See Add-AdminRight for further details.

The identifier of the new role is chosen automatically, and custom roles created with this cmdlet always have their BuiltIn flag set to false.

You cannot modify built-in roles, and only some license editions support custom roles.

Related topics

Get-AdminRole

Set-AdminRole

Rename-AdminRole

Remove-AdminRole

Set-AdminRoleMetadata

Remove-AdminRoleMetadata

Add-AdminPermission

Add-AdminRight

Parameters

-Name<String>

Specifies the name of the role. Each role in a site must have a unique name.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Specifies the description of the role.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.Role

The newly created role.

Notes

Roles are created without any permissions. Use the Add-AdminPermission to add permissions.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-AdminRole -Name Supervisor -Description "My custom supervisor role"
C:\PS> $list = Get-AdminRole 'Help Desk Administrator' | Select -Expand Permissions
C:\PS> Add-AdminPermission -Role Supervisor -Permission $list
C:\PS> Add-AdminPermission -Role Supervisor -Permission $extras
C:\PS> Add-AdminRight -Administrator DOMAIN\TestUser -Role Supervisor -All
```

Creates a new role called 'Supervisor', and then copies the permissions from the help desk role and adds some extras. Then gives this role (with the all scope) to user 'TestUser'.

New-AdminScope

Sep 10, 2014

Adds a new scope to the site.

Syntax

```
New-AdminScope [-Name] <String> [-Description <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

New-AdminScope adds a new scope object to the site.

A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to the organization; for example, the set of delivery groups used by the Sales team.

You can create objects in particular scopes by specifying the -Scope parameter of a New- cmdlet for an object that can be scoped. You can then modify the contents of a scope with Add-<Noun>Scope and Remove-<Noun>Scope cmdlets from the correpsonding PowerShell snap-ins.

To assign a scope to an administrator, combine it with a role and then assign this pair (also known as a 'right') to an administrator. See Add-AdminRight for further details.

The identifier of the new scope is chosen automatically.

Related topics

Get-AdminScope

Set-AdminScope

Rename-AdminScope

Remove-AdminScope

Set-AdminScopeMetadata

Remove-AdminScopeMetadata

Add-AdminRight

Parameters

-Name<String>

Specifies the name of the scope. Each scope in a site must have a unique name.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Specifies the description of the scope.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

None You cannot pipe input into this cmdlet.

Return Values

Citrix.DelegatedAdmin.Sdk.Scope

The newly created scope.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-AdminScope -Name Sales -Description "Sales department scope"
C:\PS> Add-HypHypervisorConnectionScope -HypervisorConnectionName XenServer2 -Scope Sales
C:\PS> Add-AdminRight -Administrator DOMAIN\TestUser -Role Hosting -Scope Sales
```

Creates a new scope called 'Sales', adds a hypervisor connection object to the scope, and then assigns the right to use the hosting role on the Sales scope to the 'TestUser' administrator.

Remove-AdminAdministrator

Sep 10, 2014

Removes administrators from the site.

Syntax

Remove-AdminAdministrator [-InputObject] <Administrator[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminAdministrator -Sid <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminAdministrator [-Name] <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Remove-AdminAdministrator cmdlet deletes administrators from the site.

Related topics

New-AdminAdministrator

Get-AdminAdministrator

Set-AdminAdministrator

Set-AdminAdministratorMetadata

Remove-AdminAdministratorMetadata

Parameters

-InputObject<Administrator[]>

Specifies the administrators to delete.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String[]>

Specifies the name of the administrator to delete.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Sid<String[]>

Specifies the SID of the administrator to delete.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Administrator You can pipe the adminstrators to be deleted into this command.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-AdminAdministrator DOMAIN\TestUser
```

Remove the administrator called "DOMAIN\TestUser".

---------- EXAMPLE 2 ----------

```
C:\PS> Get-AdminAdministrator -Enabled $false | Remove-AdminAdministrator
```

Remove all disabled administrators.

Remove-AdminAdministratorMetadata

Sep 10, 2014

Removes metadata from the given Administrator.

Syntax

```
Remove-AdminAdministratorMetadata -AdministratorSid <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminAdministratorMetadata -AdministratorSid <String> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminAdministratorMetadata [-AdministratorName] <String> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminAdministratorMetadata [-AdministratorName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminAdministratorMetadata [-InputObject] <Administrator[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminAdministratorMetadata [-InputObject] <Administrator[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Administrator.

Related topics

Set-AdminAdministratorMetadata

Parameters

-AdministratorName<String>

Name of the Administrator

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Administrator[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdministratorSid<String>

Sid of the Administrator

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-

LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminAdministrator | % { Remove-AdminAdministratorMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Administrator objects.

Remove-AdminPermission

Sep 10, 2014

Remove permissions from the set of permissions of a role.

Syntax

```
Remove-AdminPermission [-InputObject] <Permission[]> -Role <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminPermission [-Permission] <String[]> -Role <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminPermission -All -Role <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Remove permissions from the set of permissions that a role maps to.

Any administrator with a right including that role immediately loses the ability to use the operations of the removed permissions.

Duplicate permissions do not produce an error, and permissions that the roles does not already have are skipped (without error).

You cannot modify the permissions of built-in roles.

Related topics

Add-AdminPermission

Get-AdminPermission

Get-AdminRole

Get-AdminPermissionGroup

Test-AdminAccess

Parameters

-InputObject<Permission[]>

Specifies the permissions to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Permission<String[]>

Specifies the list of permissions to remove (by identifier).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Role<String>

Role name or identifier of the role to update.

Required?	true
Default Value	
Accept Pipeline Input?	false

-All<SwitchParameter>

Remove all permissions.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Permission You can pipe a list of permissions to be removed into this command.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

C:\PS> Remove-AdminPermission -Role MyRole -Permission Global_Read,Logging_Read
Remove a couple of specific permissions from the 'MyRole' role.

---------- EXAMPLE 2 ----------

C:\PS> Remove-AdminPermission -Role MyRole -All
Remove all permissions from the 'MyRole' role.

Remove-AdminRight

Sep 10, 2014

Removes rights from an administrator.

Syntax

Remove-AdminRight -Scope <String> -Role <String> -Administrator <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminRight -Role <String> -Administrator <String> [-All] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminRight [-InputObject] <Right[]> -Administrator <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

This command removes rights from the specified administrator.

For convenience, you can use the -All parameter to specify the 'All' scope.

Use the Get-AdminAdministrator cmdlet to determine what rights an administrator has.

Related topics

Get-AdminAdministrator

Get-AdminEffectiveRight

Add-AdminRight

Parameters

-InputObject<Right[]>

Specifies the rights to remove.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Scope<String>

Specifies the scope name or scope identifier.

Required?	true

Default Value	
Accept Pipeline Input?	false

-Role<String>

Specifies the role name or role identifier.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Administrator<String>

Specifies the name or SID of the administrator.

Required?	true
Default Value	
Accept Pipeline Input?	false

-All<SwitchParameter>

Specifies the 'All' scope. This parameter avoids localization issues or having to type the identifier of the 'All' scope.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Right You can pipe the rights to be removed into this command.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> RemoveAdminRight -Role 'Help Desk Administrator' -Scope London -Administrator DOMAIN\Admin1
```

Removes the 'Help Desk Administrator' role and 'London' scope from user 'Admin1'

---------- EXAMPLE 2 ----------

```
C:\PS> $admin = Get-AdminAdministrator -Name DOMAIN\Admin
C:\PS> Remove-AdminRight -InputObject $admin.Rights -Administrator DOMAIN\Admin
```

Removes all rights from administrator 'Admin'.

Remove-AdminRole

Sep 10, 2014

Removes a role from the site.

Syntax

```
Remove-AdminRole [-InputObject] <Role[]> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminRole [-Id] <Guid[]> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminRole [-Name] <String[]> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-AdminRole cmdlet deletes roles from the site.

You cannot remove built-in roles.

An error will be produced if the role being removed is currently assigned to an administrator unless you specify the -Force option. When -Force is specified, any rights that reference the role are also removed.

Related topics

New-AdminRole

Get-AdminRole

Set-AdminRole

Rename-AdminRole

Set-AdminRoleMetadata

Remove-AdminRoleMetadata

Parameters

-InputObject<Role[]>

Specifies the roles to remove (by role object).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Id<Guid[]>

Specifies the roles to remove (by role id).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Name<String[]>

Specifies the roles to remove (by role name).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Force<SwitchParameter>

Allow removal of roles that are still in use.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Role You can pipe the roles to be deleted into this command.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-AdminRole -Name Supervisor
```

Remove the Supervisor role.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-AdminRole -BuiltIn $false | Remove-AdminRole
```

Attempt to remove all custom roles. This fails if one of the roles is assigned to an administrator.

Remove-AdminRoleMetadata

Sep 10, 2014

Removes metadata from the given Role.

Syntax

```
Remove-AdminRoleMetadata [-RoleId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminRoleMetadata [-RoleId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminRoleMetadata [-RoleName] <String> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminRoleMetadata [-RoleName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminRoleMetadata [-InputObject] <Role[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminRoleMetadata [-InputObject] <Role[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Role.

Related topics

Set-AdminRoleMetadata

Parameters

-RoleId<Guid>

Id of the Role

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-RoleName<String>

Name of the Role

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Role[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-

LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminRole | % { Remove-AdminRoleMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Role objects.

Remove-AdminScope

Sep 10, 2014

Removes a scope from the site.

Syntax

```
Remove-AdminScope [-InputObject] <Scope[]> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminScope [-Id] <Guid[]> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminScope [-Name] <String[]> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Remove-AdminScope cmdlet deletes scopes from the site.

You cannot remove the built-in 'All' scope.

An error will be produced if the scope being removed is currently assigned to an administrator unless you specify the -Force option. When -Force is specified, any rights that reference the scope are also removed.

Related topics

New-AdminScope

Get-AdminScope

Set-AdminScope

Rename-AdminScope

Set-AdminScopeMetadata

Remove-AdminScopeMetadata

Parameters

-InputObject<Scope[]>

Specifies the scopes to remove (by scope object).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Id<Guid[]>

Specifies the scopes to remove (by scope id).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Name<String[]>

Specifies the scopes to remove (by scope name).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Force<SwitchParameter>

Allow removal of scopes that are still in use.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Scope You can pipe the scopes to be deleted into this command.

Return Values

None

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Remove-AdminScope -Name Sales
```

Remove the Sales scope.

---------- EXAMPLE 2 ----------

```
C:\PS> Get-AdminScope -BuiltIn $false | Remove-AdminScope
```

Attempt to remove all scopes (excluding the built-in 'All' scope). This fails if one of the scopes is assigned to an administrator.

Remove-AdminScopeMetadata

Sep 10, 2014

Removes metadata from the given Scope.

Syntax

```
Remove-AdminScopeMetadata [-ScopeId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminScopeMetadata [-ScopeId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminScopeMetadata [-ScopeName] <String> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminScopeMetadata [-ScopeName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminScopeMetadata [-InputObject] <Scope[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminScopeMetadata [-InputObject] <Scope[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Scope.

Related topics

Set-AdminScopeMetadata

Parameters

-ScopeId<Guid>

Id of the Scope

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ScopeName<String>

Name of the Scope

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Scope[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-

LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminScope | % { Remove-AdminScopeMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Scope objects.

Remove-AdminServiceMetadata

Sep 10, 2014

Removes metadata from the given Service.

Syntax

```
Remove-AdminServiceMetadata [-ServiceHostId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminServiceMetadata [-InputObject] <Service[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-AdminServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Service.

Related topics

Set-AdminServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-AdminService | % { Remove-AdminServiceMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Service objects.

Rename-AdminRole

Sep 10, 2014

Rename a role

Syntax

```
Rename-AdminRole [-InputObject] <Role> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-AdminRole [-Id] <Guid> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-AdminRole [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-AdminRole cmdlet changes the name of a role.

Role names must be unique, and you cannot modify the name of built-in roles.

Related topics

New-AdminRole

Get-AdminRole

Set-AdminRole

Remove-AdminRole

Set-AdminRoleMetadata

Remove-AdminRoleMetadata

Parameters

-InputObject<Role>

Specifies the role to rename (by object).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Id<Guid>

Specifies the role to rename (by id).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Name<String>

Specifies the role to rename (by name).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

Specifies the new name of the role.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Returns the affected record. By default, this cmdlet does not generate any output.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create

high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Role You can pipe the role to be renamed into this command.

Return Values

None or Citrix.DelegatedAdmin.Sdk.Role

When you use the PassThru parameter, Rename-AdminRole generates a Citrix.DelegatedAdmin.Sdk.Role object. Otherwise, this cmdlet does not generate any output.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-AdminRole -Name Supervisor -NewName HelpDeskLead
```

Renames the 'Supervisor' role to 'HelpDeskLead'.

Rename-AdminScope

Sep 10, 2014

Rename a scope

Syntax

```
Rename-AdminScope [-InputObject] <Scope> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-AdminScope [-Id] <Guid> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-AdminScope [-Name] <String> [-NewName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Rename-AdminScope cmdlet changes the name of a scope.

Scope names must be unique, and you cannot modify the name of the built-in 'All' scope.

Related topics

New-AdminScope

Get-AdminScope

Set-AdminScope

Remove-AdminScope

Set-AdminScopeMetadata

Remove-AdminScopeMetadata

Parameters

-InputObject<Scope>

Specifies the scope to rename (by object).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Id<Guid>

Specifies the scope to rename (by id).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Name<String>

Specifies the scope to rename (by name).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-NewName<String>

Specifies the new name of the scope.

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Returns the affected record. By default, this cmdlet does not generate any output.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create

high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Scope You can pipe the scope to be renamed into this command.

Return Values

None or Citrix.DelegatedAdmin.Sdk.Scope

When you use the PassThru parameter, Rename-AdminScope generates a Citrix.DelegatedAdmin.Sdk.Scope object. Otherwise, this cmdlet does not generate any output.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Rename-AdminScope -Name Sales -NewName SalesDesktops
```

Renames the 'Sales' scope to 'SalesDesktops'.

Reset-AdminServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the DelegatedAdmin Service.

Syntax

```
Reset-AdminServiceGroupMembership [-ConfigServiceInstance] <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables you to reload DelegatedAdmin Service access permissions and configuration service locations. The Reset-AdminServiceGroupMembership command must be run on at least one instance of the service type (Admin) after installation and registration with the configuration service. Without this operation, the DelegatedAdmin services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-AdminServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Parameters

-ConfigServiceInstance<ServiceInstance[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-AdminServiceGroupMembership command.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-AdminServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-AdminServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Set-AdminAdministrator

Sep 10, 2014

Sets the properties of an administrator.

Syntax

```
Set-AdminAdministrator [-InputObject] <Administrator[]> [-Enabled <Boolean>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminAdministrator -Sid <String[]> [-Enabled <Boolean>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminAdministrator [-Name] <String[]> [-Enabled <Boolean>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The Set-AdminAdministrator cmdlet is used to enable or disable an existing administrator.

You can specify the administrators to modify in a number of ways, by piping in existing objects, by passing existing objects with the InputObject parameter, or by specifying the names or SIDs explicitly.

Related topics

New-AdminAdministrator

Get-AdminAdministrator

Remove-AdminAdministrator

Set-AdminAdministratorMetadata

Remove-AdminAdministratorMetadata

Parameters

-InputObject<Administrator[]>

Specifies the administrators to modify.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String[]>

Specifies the names of the administrators to modify.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Sid<String[]>

Specifies the SIDs of the administrators to modify.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Enabled<Boolean>

Specifies the new value for the Enabled property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Returns the affected record. By default, this cmdlet does not generate any output.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Administrator You can pipe the adminstrators to be modified into this command.

Return Values

None or Citrix.DelegatedAdmin.Sdk.Administrator

When you use the PassThru parameter, Set-AdminAdministrator generates a Citrix.DelegatedAdmin.Sdk.Administrator object. Otherwise, this cmdlet does not generate any output.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Get-AdminAdministrator -Enabled $false | Set-AdminAdministrator -Enabled $true
```

Enable all administrators that are currently disabled.

---------- EXAMPLE 2 ----------

```
C:\PS> Set-AdminAdministrator -Name DOMAIN\TestUser1,DOMAIN\TestUser2 -Enabled $true
```

Enable two specific users specified by name (TestUser1 and TestUser2).

Set-AdminAdministratorMetadata

Sep 10, 2014

Adds or updates metadata on the given Administrator.

Syntax

Set-AdminAdministratorMetadata -AdministratorSid <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminAdministratorMetadata -AdministratorSid <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminAdministratorMetadata [-AdministratorName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminAdministratorMetadata [-AdministratorName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminAdministratorMetadata [-InputObject] <Administrator[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminAdministratorMetadata [-InputObject] <Administrator[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given Administrator objects.

Related topics

Remove-AdminAdministratorMetadata

Parameters

-AdministratorName<String>

Name of the Administrator

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Administrator[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdministratorSid<String>

Sid of the Administrator

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Administrator specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-AdminAdministratorMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-AdminAdministratorMetadata -AdministratorSid S-1-5-21-1505241163-3345470479-1241728991-1000 -Name property -Value value

      Key                            Value
      ---                            -----
      property                           value
```

Add metadata with a name of 'property' and a value of 'value' to the Administrator with the identifier 'S-1-5-21-1505241163-3345470479-1241728991-1000'.

Set-AdminDBConnection

Sep 10, 2014

Configures a database connection for the DelegatedAdmin Service.

Syntax

```
Set-AdminDBConnection [-DBConnection] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Configures a connection to a database in which the DelegatedAdmin Service can store its state. The service will attempt to connect and start using the database immediately after the connection is configured. The database connection string is updated to the specified value regardless of whether it is valid or not. Specifying an invalid connection string prevents a service from functioning until the error is corrected.

After a connection is configured, you cannot alter it without first clearing it (by setting the connection to $null).

You do not need to configure a database connection to use this command.

Related topics

Get-AdminServiceStatus

Get-AdminDBConnection

Test-AdminDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the DelegatedAdmin Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-AdminDBConnection command returns an object containing the status of the DelegatedAdmin Service together with extra diagnostics information.

DBUnconfigured

The DelegatedAdmin Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the DelegatedAdmin Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the DelegatedAdmin Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the DelegatedAdmin Service currently in use is incompatible with the version of the DelegatedAdmin Service schema on the database. Upgrade the DelegatedAdmin Service to a more recent version.

DBOlderVersionThanService

The version of the DelegatedAdmin Service schema on the database is incompatible with the version of the DelegatedAdmin Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The DelegatedAdmin Service is running and is connected to a database containing a valid schema.

Failed

The DelegatedAdmin Service has failed.

Unknown

The status of the DelegatedAdmin Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-AdminDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Configures a database connection string for the DelegatedAdmin Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Set-AdminDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Configures an invalid database connection string for the DelegatedAdmin Service.

Set-AdminRole

Sep 10, 2014

Set the properties of a role.

Syntax

Set-AdminRole [-InputObject] <Role[]> [-Description <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminRole [-Id] <Guid[]> [-Description <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminRole [-Name] <String[]> [-Description <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-AdminRole command allows the description of custom roles to be updated. You cannot modify built-in roles.

To modify the permissions of a role, use the Add-AdminPermission and Remove-AdminPermission cmdlets.

To update the metadata associated with a role, use the Set-AdminRoleMetadata and Remove-AdminRoleMetadata cmdlets.

Related topics

New-AdminRole

Get-AdminRole

Remove-AdminRole

Rename-AdminRole

Set-AdminRoleMetadata

Remove-AdminRoleMetadata

Add-AdminPermission

Remove-AdminPermission

Parameters

-InputObject<Role[]>

Specifies the roles to update (by object).

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-Id<Guid[]>

Specifies the roles to update (by id).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Name<String[]>

Specifies the roles to update (by name).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Supplies the new description value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Returns the affected record. By default, this cmdlet does not generate any output.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Role You can pipe the roles to be updated into this command.

Return Values

None or Citrix.DelegatedAdmin.Sdk.Role

When you use the PassThru parameter, Set-AdminRole generates a Citrix.DelegatedAdmin.Sdk.Role object. Otherwise, this cmdlet does not generate any output.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-AdminRole -Name Supervisor -Description "Helpdesk supervisor role"
```

Change the description of the 'Supervisor' role.

Set-AdminRoleMetadata

Sep 10, 2014

Adds or updates metadata on the given Role.

Syntax

Set-AdminRoleMetadata [-RoleId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminRoleMetadata [-RoleId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminRoleMetadata [-RoleName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminRoleMetadata [-RoleName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminRoleMetadata [-InputObject] <Role[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminRoleMetadata [-InputObject] <Role[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given Role objects.

Related topics

Remove-AdminRoleMetadata

Parameters

-RoleId<Guid>

Id of the Role

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-RoleName<String>

Name of the Role

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Role[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Role specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-AdminRoleMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-AdminRoleMetadata -RoleId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

    Key                            Value
    ---                            -----
    property                           value
```

Add metadata with a name of 'property' and a value of 'value' to the Role with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-AdminScope

Sep 10, 2014

Set the properties of a scope.

Syntax

Set-AdminScope [-InputObject] <Scope[]> [-Description <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminScope [-Id] <Guid[]> [-Description <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminScope [-Name] <String[]> [-Description <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The Set-AdminScope command allows the description of scopes to be updated. You cannot modify the built-in 'All' scope.

To change the contents of a scope, use the Add-<Noun>Scope and Remove-<Noun>Scope cmdlets from the corresponding PowerShell snap-in.

To update the metadata associated with a scope, use the Set-AdminScopeMetadata and Remove-AdminScopeMetadata cmdlets.

Related topics

New-AdminScope

Get-AdminScope

Remove-AdminScope

Rename-AdminScope

Set-AdminScopeMetadata

Remove-AdminScopeMetadata

Parameters

-InputObject<Scope[]>

Specifies the scopes to update (by object).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Id<Guid[]>

Specifies the scopes to update (by id).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Name<String[]>

Specifies the scopes to update (by name).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Supplies the new description value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Returns the affected record. By default, this cmdlet does not generate any output.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.DelegatedAdmin.Sdk.Scope You can pipe the scopes to be updated into this command.

Return Values

None or Citrix.DelegatedAdmin.Sdk.Scope

When you use the PassThru parameter, Set-AdminScope generates a Citrix.DelegatedAdmin.Sdk.Scope object. Otherwise, this cmdlet does not generate any output.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-AdminScope -Name Sales -Description "Sales department desktops"
```

Change the description of the 'Sales' scope.

Set-AdminScopeMetadata

Sep 10, 2014

Adds or updates metadata on the given Scope.

Syntax

Set-AdminScopeMetadata [-ScopeId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminScopeMetadata [-ScopeId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminScopeMetadata [-ScopeName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminScopeMetadata [-ScopeName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminScopeMetadata [-InputObject] <Scope[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminScopeMetadata [-InputObject] <Scope[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given Scope objects.

Related topics

Remove-AdminScopeMetadata

Parameters

-ScopeId<Guid>

Id of the Scope

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ScopeName<String>

Name of the Scope

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Scope[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Scope specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-AdminScopeMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-AdminScopeMetadata -ScopeId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                         Value
        ---                         -----
        property                        value
```

Add metadata with a name of 'property' and a value of 'value' to the Scope with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-AdminServiceMetadata

Sep 10, 2014

Adds or updates metadata on the given Service.

Syntax

Set-AdminServiceMetadata [-ServiceHostId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-AdminServiceMetadata [-InputObject] <Service[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Allows you to store additional custom data against given Service objects.

Related topics

Remove-AdminServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Service specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true

Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-AdminServiceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------


```
c:\PS>Set-AdminServiceMetadata -ServiceHostId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Service with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Test-AdminAccess

Sep 10, 2014

Retrieves the scopes where the specified operation is permitted.

Syntax

```
Test-AdminAccess [-Operation] <String[]> [-Annotate] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This cmdlet evaluates what rights the current user has, and from these determines the scopes where the specified operation is permitted.

Operations are the indivisible unit of functionality that each XenDesktop service can perform, and usually correspond to individual cmdlets.

If you specify the -Annotate option or specify multiple operations to check, the resulting object is annotated with the operation the result relates to.

Related topics

Parameters

-Operation<String[]>

The operation to query.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Annotate<SwitchParameter>

Annotates each result with the operation it relates to.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name

or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.DelegatedAdmin.Sdk.ScopeReference

The list of permissible scopes for the specified single operation.PSObject

The list of permissible scopes for each operation. This type of object is returned when the -Annotate option or multiple operations are specified.

Notes

If the specified operation has unrestricted access a single object is returned representing the 'All' scope with a ScopeId of Guid.Empty (00000000-0000-0000-0000-000000000000).

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Test-AdminAccess -Operation 'Broker:GetCatalog'
```

Queries the scopes where 'Broker:GetCatalog' is permitted.

---------- EXAMPLE 2 ----------

```
C:\PS> Test-AdminAccess -Operation 'Broker:GetCatalog','Broker:GetMachine'
```

Queries the scopes where 'Broker:GetCatalog' or 'Broker:GetMachine' are permitted.

Test-AdminDBConnection

Sep 10, 2014

Tests a database connection for the DelegatedAdmin Service.

Syntax

```
Test-AdminDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Tests a connection to the database in which the DelegatedAdmin Service can store its state. The service will attempt to connect to the database without affecting the current connection to the database.

You do not have to clear the connection to use this command.

Related topics

Get-AdminServiceStatus

Get-AdminDBConnection

Set-AdminDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the DelegatedAdmin Service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-AdminDBConnection command returns an object containing the status of the DelegatedAdmin Service if the connection string of the specified data store were to be set to the string being tested, together with extra diagnostics information for the specified connection string.

DBRejectedConnection

The database rejected the logon attempt from the DelegatedAdmin Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the DelegatedAdmin Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the DelegatedAdmin Service currently in use is incompatible with the version of the DelegatedAdmin Service schema on the database. Upgrade the DelegatedAdmin Service to a more recent version.

DBOlderVersionThanService

The version of the DelegatedAdmin Service schema on the database is incompatible with the version of the DelegatedAdmin Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Set-AdminDBConnection command would succeed if it were executed with the supplied connection string.

Failed

The DelegatedAdmin Service has failed.

Unknown

The status of the DelegatedAdmin Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Test-AdminDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"
```


OK
Tests a database connection string for the DelegatedAdmin Service.

---------- EXAMPLE 2 ----------

c:\PS>Test-AdminDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
Tests an invalid database connection string for the DelegatedAdmin Service.

Citrix.EnvTest.Admin.V1

Aug 31, 2016

Overview

Name	Description
EnvTestEnvTestSnapin	The Citrix Environment Test Service provides tools to test and inspect the state of a XenDesktop installation.
EnvTest Filtering	Describes the common filtering options for XenDesktop cmdlets.

Cmdlets

Name	Description
Get-EnvTestConfiguration	Gets the Environment Test Service's configuration options
Get-EnvTestDBConnection	Gets the database string for the specified data store used by the EnvTest Service.
Get-EnvTestDBSchema	Gets a script that creates the EnvTest Service database schema for the specified data store.
Get-EnvTestDBVersionChangeScript	Gets a script that updates the EnvTest Service database schema.
Get-EnvTestDefinition	Gets the one or more test definitions
Get-EnvTestInstalledDBVersion	Gets a list of all available database schema versions for the EnvTest Service.
Get-EnvTestService	Gets the service record entries for the EnvTest Service.
Get-EnvTestServiceAddedCapability	Gets any added capabilities for the EnvTest Service on the controller.
Get-EnvTestServiceInstance	Gets the service instance entries for the EnvTest Service.
Get-EnvTestServiceStatus	Gets the current status of the EnvTest Service on the controller.
Get-EnvTestSuiteDefinition	Gets one or more test suite definitions.
Get-EnvTestTask	Gets one or more EnvTestTask(s)

Name	Description
New-EnvTestDiscoveryTargetDefinition	Creates a new EnvTestDiscoveryTargetDefinition object
Remove-EnvTestServiceMetadata	Removes metadata from the given Service.
Remove-EnvTestTask	Removes from the database completed tasks for the EnvTest Service.
Remove-EnvTestTaskMetadata	Removes metadata from the given Task.
Reset-EnvTestServiceGroupMembership	Reloads the access permissions and configuration service locations for the EnvTest Service.
Set-EnvTestConfiguration	Sets the Environment Test Service's configuation options
Set-EnvTestDBConnection	Configures a database connection for the EnvTest Service.
Set-EnvTestServiceMetadata	Adds or updates metadata on the given Service.
Set-EnvTestTaskMetadata	Adds or updates metadata on the given Task.
Start-EnvTestTask	Starts a new test task.
Stop-EnvTestTask	Stops a still running task from completing.
Switch-EnvTestTask	Sets the current task that will be returned by a call to Get-EnvTestTask with no parameters.
Test-EnvTestDBConnection	Tests a database connection for the EnvTest Service.

about_EnvTestEnvTestSnapin

Sep 10, 2014

TOPIC

about_EnvTestEnvTestSnapin

SHORT DESCRIPTION

The Citrix Environment Test Service provides tools to test and inspect the state of a XenDesktop installation.

COMMAND PREFIX

All commands in this snap-in have the noun prefixed with 'EnvTest'.

LONG DESCRIPTION

The Citrix Environment Test Service provides tools to test and inspect the state of a XenDesktop installation at different points during and after configuration and install.

about_EnvTest_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more
are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```

retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

A120901
B220000
...

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

Get-EnvTestConfiguration

Sep 10, 2014

Gets the Environment Test Service's configuation options

Syntax

```
Get-EnvTestConfiguration [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets the Environment Test Service's configuation options and returns them as key/value pairs.

Related topics

Parameters

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Dictionary<string, object>

All configuration settings

Examples

---------- EXAMPLE 1 ----------

Get-EnvTestConfiguration
Gets all configuration options

Get-EnvTestDBConnection

Sep 10, 2014

Gets the database string for the specified data store used by the EnvTest Service.

Syntax

```
Get-EnvTestDBConnection [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the database connection string for the specified data store.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

Related topics

Get-EnvTestServiceStatus

Set-EnvTestDBConnection

Test-EnvTestDBConnection

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

system.string

The database connection string configured for the EnvTest Service.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the EnvTest Service has not been specified.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-EnvTestDBConnection

Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True
```

Get the database connection string for the EnvTest Service.

Get-EnvTestDBSchema

Sep 10, 2014

Gets a script that creates the EnvTest Service database schema for the specified data store.

Syntax

Get-EnvTestDBSchema [-DatabaseName <String>] [-ServiceGroupName <String>] [-ScriptType <ScriptTypes>] [-LocalDatabase] [-Sid <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets SQL scripts that can be used to create a new EnvTest Service database schema, add a new EnvTest Service to an existing site, remove a EnvTest Service from a site, or create a database server logon for a EnvTest Service. If no Sid parameter is provided, the scripts obtained relate to the currently selected EnvTest Service instance, otherwise the scripts relate to EnvTest Service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied. The current service instance is that on the local machine, or that explicitly specified by the last usage of the -AdminAddress parameter to a EnvTest SDK cmdlet. The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured. The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SMDCMD mode'. The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to EnvTest Service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to EnvTest Service roles

If ScriptType is Evict, the returned script contains:

o Removal of EnvTest Service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database. You do not need to configure a database before using this command.

Related topics

Set-EnvTestDBConnection

Parameters

-DatabaseName<String>

Specifies the name of the database for which the schema will be generated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the EnvTest services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<ScriptTypes>

Specifies the type of database script returned. Available script types are:

Database

Returns a full database script that can be used to create a database schema for the EnvTest Service in a database instance that does not already contain a schema for this service. The DatabaseName and ServiceGroupName parameters must be specified to create a script of this type.

Instance

Returns a permissions script that can be used to add further EnvTest services to an existing database instance that already contains the full EnvTest service schema, associating the services to the Service Group. The Sid parameter can optionally be specified to create a script of this type.

Login

Returns a database logon script that can be used to add the required logon accounts to an existing database instance that contains the EnvTest Service schema. This is used primarily when creating a mirrored database environment. The DatabaseName parameter must be specified to create a script of this type.

Evict

Returns a script that can be used to remove the specified EnvTest Service from the database entirely. The DatabaseName and Sid parameters must be specified to create a script of this type.

Required?	false
Default Value	Database
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for EnvTest services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Sid<String>

Specifies the SID of the controller on which the EnvTest Service instance to remove from the database is running.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.string

A string containing the required SQL script for application to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-EnvTestDBSchema -DatabaseName MyDB -ServiceGroupName  MyServiceGroup > c:\EnvTestSchema.sql
```

Get the full database schema for site data store of the EnvTest Service and copy it to a file called 'c:\EnvTestSchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a EnvTest Service site schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-EnvTestDBSchema -DatabaseName MyDB -scriptType Login > c:\EnvTestLogins.sql
```

Get the logon scripts for the EnvTest Service.

Get-EnvTestDBVersionChangeScript

Sep 10, 2014

Gets a script that updates the EnvTest Service database schema.

Syntax

```
Get-EnvTestDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a database script that can be used to upgrade or downgrade the site or secondary schema for the EnvTest Service from the current schema version to a different version.

Related topics

Get-EnvTestInstalledDBVersion

Parameters

-DatabaseName<String>

Specifies the name of the database instance to which the update applies.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

Specifies the version of the database you want to update to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

A PSObject containing the required SQL script for application to a database.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any EnvTest services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-EnvTestServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the EnvTest Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $update = Get-EnvTestDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-EnvTestDefinition

Sep 10, 2014

Gets the one or more test definitions

Syntax

```
Get-EnvTestDefinition [-TestId <String[]>] [-CultureName <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a list of test definitions that are available from currently running components.

Related topics

Get-EnvTestSuiteDefinition

Get-EnvTestTask

Start-EnvTestTask

Switch-EnvTestTask

Stop-EnvTestTask

Remove-EnvTestTask

Add-EnvTestTaskMetadata

Remove-EnvTestTaskMetadata

Parameters

-TestId<String[]>

The id of one or more tests.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-CultureName<String>

The culture name in which to produce results. The culture name is in standard language/region-code format; for example "en-US".

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.String A test id. System.String[] An array of test ids.

Return Values

Citrix.EnvTest.Sdk.EnvTestDefinition

One or more test definitions.

Examples

---------- EXAMPLE 1 ----------

```
$allTestDefinitions = Get-EnvTestDefinition
```

Retrieve all tests.

---------- EXAMPLE 2 ----------

```
$allTestDefinitionsTranslatedIntoSpanish = Get-EnvTestDefinition -CultureName es-ES
```

Retrieve all tests with localized properties returned in Spanish.

---------- EXAMPLE 3 ----------

```
$monitorConfigServiceRegistrationDefinition = Get-EnvTestDefinition -TestId Monitor_RegisteredWithConfigurationService
```

Retrieve the definition of the 'Monitor_RegisteredWithConfigurationService' test.

Get-EnvTestInstalledDBVersion

Sep 10, 2014

Gets a list of all available database schema versions for the EnvTest Service.

Syntax

```
Get-EnvTestInstalledDBVersion [-Upgrade] [-Downgrade] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Returns the current version of the EnvTest Service database schema, if no flags are set, otherwise returns versions for which upgrade or downgrade scripts are available and have been stored in the database.

Related topics

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Version

The Get-EnvTestInstalledDbVersion command returns objects containing the new definition of the EnvTest Service database schema version.

Major <Integer>

Minor <Integer>

Build <Integer>

Revision <Integer>

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the EnvTest Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-EnvTestInstalledDBVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      6      0      0
```

Get the currently installed version of the EnvTest Service database schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-EnvTestInstalledDBVersion -Upgrade

Major  Minor  Build  Revision
-----  -----  -----  --------
6      0      0      0
```

Get the versions of the EnvTest Service database schema for which upgrade scripts are supplied.

Get-EnvTestService

Sep 10, 2014

Gets the service record entries for the EnvTest Service.

Syntax

```
Get-EnvTestService [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns instances of the EnvTest Service that the service publishes. The service records contain account security identifier information that can be used to remove each service from the database.

A database connection for the service is required to use this command.

Related topics

Parameters

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_EnvTest_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_EnvTest_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.EnvTest.Sdk.Service

The Get-EnvTestServiceInstance command returns an object containing the following properties.

Uid <Integer>

Specifies the unique identifier for the service in the group. The unique identifier is an index number.

ServiceHostId <Guid>

Specifies the unique identifier for the service instance.

DNSName <String>

Specifies the domain name of the host on which the service runs.

MachineName <String>

Specifies the short name of the host on which the service runs.

CurrentState <Citrix.Fma.Sdk.ServiceCore.ServiceState>

Specifies whether the service is running, started but inactive, stopped, or failed.

LastStartTime <DateTime>

Specifies the date and time at which the service was last restarted.

LastActivityTime <DateTime>

Specifies the date and time at which the service was last stopped or restarted.

OSType

Specifies the operating system installed on the host on which the service runs.

OSVersion

Specifies the version of the operating system installed on the host on which the service runs.

ServiceVersion

Specifies the version number of the service instance. The version number is a string that reflects the full build version of the service.

DatabaseUserName <string>

Specifies for the service instance the Active Directory account name with permissions to access the database. This will be either the machine account or, if the database is running on a controller, the NetworkService account.

Sid <string>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

ActiveSiteServices <string[]>

Specifies the names of active site services currently running in the service. Site services are components that perform long-running background processing in some services. This field is empty for services that do not contain site services.

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-EnvTestService

Uid             : 1
ServiceHostId   : aef6f464-f1ee-4042-a523-66982e0cecd0
DNSName         : MyServer.company.com
MachineName     : MYSERVER
CurrentState    : On
LastStartTime   : 04/04/2011 15:25:38
LastActivityTime : 04/04/2011 15:33:39
OSType          : Win32NT
OSVersion       : 6.1.7600.0
ServiceVersion  : 5.1.0.0
DatabaseUserName : NT AUTHORITY\NETWORK SERVICE
SID             : S-1-5-21-2316621082-1546847349-2782505528-1165
ActiveSiteServices : {MySiteService1, MySiteService2...}
```

Get all the instances of the EnvTest Service running in the current service group.

Get-EnvTestServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the EnvTest Service on the controller.

Syntax

```
Get-EnvTestServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the EnvTest Service on the controller to be detected.

You do not need to configure a database connection before using this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-EnvTestServiceAddedCapability
```

Get the added capabilities of the EnvTest Service.

Get-EnvTestServiceInstance

Sep 10, 2014

Gets the service instance entries for the EnvTest Service.

Syntax

```
Get-EnvTestServiceInstance [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns service interfaces published by the instance of the EnvTest Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.EnvTest.Sdk.ServiceInstance

The Get-EnvTestServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a

central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

Specifies the service instance type. For this service, the service instance type is always EnvTest.

Address

Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

SDK - for PowerShell operations

InterService - for operations between different services

Peer - for communications between services of the same type

Metadata <Citrix.EnvTest.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-EnvTestServiceInstance

Address          : http://MyServer.com:80/Citrix/EnvTestContract
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         :
MetadataMap      :
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName  : MyServiceGroup
ServiceGroupUid   : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType      : EnvTest
Version          : 1

Address          : http://MyServer.com:80/Citrix/EnvTestContract/IServiceApi
Binding          : wcf_HTTP_kerb
InterfaceType    : InterService
Metadata         :
MetadataMap      :
```



```
ServiceAccount     : ENG\MyAccount
ServiceAccountSid  : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName   : MyServiceGroup
ServiceGroupUid    : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType        : EnvTest
Version            : 1
```

Get all instances of the EnvTest Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-EnvTestServiceStatus

Sep 10, 2014

Gets the current status of the EnvTest Service on the controller.

Syntax

```
Get-EnvTestServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the EnvTest Service on the controller to be monitored. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured.

Related topics

Set-EnvTestDBConnection

Test-EnvTestDBConnection

Get-EnvTestDBConnection

Get-EnvTestDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-EnvTestServiceStatus command returns an object containing the status of the EnvTest Service together with extra diagnostics information.

DBUnconfigured

The EnvTest Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the EnvTest Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the EnvTest Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the EnvTest Service currently in use is incompatible with the version of the EnvTest Service schema on the database. Upgrade the EnvTest Service to a more recent version.

DBOlderVersionThanService

The version of the EnvTest Service schema on the database is incompatible with the version of the EnvTest Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The EnvTest Service is running and is connected to a database containing a valid schema.

Failed

The EnvTest Service has failed.

Unknown

(0) The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-EnvTestServiceStatus
```

DBUnconfigured
Get the current status of the EnvTest Service.

Get-EnvTestSuiteDefinition

Sep 10, 2014

Gets one or more test suite definitions.

Syntax

Get-EnvTestSuiteDefinition [-TestSuiteId <String[]>] [-CultureName <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns a list of test suite definitions that are available from currently running components.

Related topics

Get-EnvTestDefinition

Get-EnvTestTask

Start-EnvTestTask

Switch-EnvTestTask

Stop-EnvTestTask

Remove-EnvTestTask

Add-EnvTestTaskMetadata

Remove-EnvTestTaskMetadata

Parameters

-TestSuiteId<String[]>

The id of one or more test suites.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-CultureName<String>

The culture name in which to produce results. The culture name is in standard language/region-code format; for example "en-US".

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.String A test suite id. System.String[] An array of test suite ids.

Return Values

Citrix.EnvTest.Sdk.EnvTestSuiteDefinition

The definition of a test suite

Examples

---------- EXAMPLE 1 ----------

```
$allTestSuiteDefinitions = Get-EnvTestSuiteDefinition
```

Retrieve all test suites.

---------- EXAMPLE 2 ----------

```
$allTestSuiteDefinitionsTranslatedIntoSpanish = Get-EnvTestSuiteDefinition -CultureName es-ES
```

Retrieve all test suites with localized properties returned in Spanish.

---------- EXAMPLE 3 ----------

```
$infrastructureSuiteDefinition = Get-EnvTestSuiteDefinition -TestSuiteId Infrastructure
```

Retrieve the definition of the 'Infrastructure' test suite.

Get-EnvTestTask

Sep 10, 2014

Gets one or more EnvTestTask(s)

Syntax

```
Get-EnvTestTask [-TaskId <Guid>] [-List] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns either the current task, a specified task, or list of tasks that are currently known to the EnvTest Service.

Related topics

Get-EnvTestDefinition

Get-EnvTestSuiteDefinition

Start-EnvTestTask

Switch-EnvTestTask

Stop-EnvTestTask

Remove-EnvTestTask

Add-EnvTestTaskMetadata

Remove-EnvTestTaskMetadata

Parameters

-TaskId<Guid>

Specifies the task identifier to be returned. This value can be retrieved from an existing task's $task.TaskId property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-List<SwitchParameter>

List all running tasks, including the current one.

Required?	false
Default Value	false

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.EnvTest.Sdk.EnvTestTask

A description of a previously started task.

Examples

---------- EXAMPLE 1 ----------

```
$currentTask = Get-EnvTestTask
```

Retrieve the current task. The current task is the most recently created task unless Switch-EnvTestTask explicitly changes it.

---------- EXAMPLE 2 ----------

```
$taskOfSpecificId = Get-EnvTestTask -TaskId 36C0EC52-2039-4D6E-B690-9F02F8CEFFCC
```

Retrieve a fresh copy of a task object based on a known task id, which is always a Guid. This id can be retrieved from an existing task object via its $task.TaskId property.

---------- EXAMPLE 3 ----------

```
$allKnownTasks = Get-EnvTestTask -List
```

Retrieve the list of current tasks. This list includes any task started by the Start-EnvTestTask cmdlet since the service started that has not later been removed via Remove-EnvTestTask.

New-EnvTestDiscoveryTargetDefinition

Sep 10, 2014

Creates a new EnvTestDiscoveryTargetDefinition object

Syntax

```
New-EnvTestDiscoveryTargetDefinition -TestId <String> [-TargetIdType <String>] [-TargetId <String>] [-AdminAddress <String>] [<CommonParameters>]
```

```
New-EnvTestDiscoveryTargetDefinition -TestSuiteId <String> [-TargetIdType <String>] [-TargetId <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Creates a new EnvTestDiscoveryTargetDefinition object that can be piped into Start-EnvTestTask to define one or more targets of execution, optionally including root objects for discovery.

Related topics

Get-EnvTestDefinition

Get-EnvTestSuiteDefinition

Get-EnvTestTask

Start-EnvTestTask

Switch-EnvTestTask

Stop-EnvTestTask

Remove-EnvTestTask

Add-EnvTestTaskMetadata

Remove-EnvTestTaskMetadata

Parameters

-TestId<String>

Test identifiers. If specified, do not specify -TestSuiteId.

Required?	true
Default Value	Empty
Accept Pipeline Input?	false

-TestSuiteId<String>

Test suite identifiers. If specified, do not specify -TestId.

Required?	true
Default Value	Empty
Accept Pipeline Input?	false

-TargetIdType<String>

Describes the type of corresponding object passed with -TargetId

Required?	false
Default Value	Empty

Accept Pipeline Input?	false

-TargetId<String>

The Ids that object tests or test suites will target. By default, other components are queried for objects related to these.

Required?	false
Default Value	Empty
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.EnvTest.Sdk.EnvTestDiscoveryTargetDefinition

Defines a target of a task

Examples

---------- EXAMPLE 1 ----------

```
$singleSimpleTestTaskTarget = New-EnvTestDiscoveryTargetDefinition -TestId Monitor_RegisteredWithConfigurationService
$singleSimpleTestTaskTarget | Start-EnvTestTask
```

Create a discovery target definition with a single test and no target object, then start a task based on it.

---------- EXAMPLE 2 ----------

```
$singleSimpleTestSuiteTaskTarget = New-EnvTestDiscoveryTargetDefinition -TestSuiteId Infrastructure
$singleSimpleTestSuiteTaskTarget | Start-EnvTestTask
```

Create a discovery target definition with a single test suite and no target object, then start a task based on it.

---------- EXAMPLE 3 ----------

```
$singleTestSuiteTaskTarget = New-EnvTestDiscoveryTargetDefinition -TestSuiteId Catalog -TargetIdType Catalog -TargetId $(Get-BrokerCatalog).Uuid
$singleTestSuiteTaskTarget | Start-EnvTestTask
```

Create a discovery target definition with a single test suite and a catalog target object, then start a task based on it.

---------- EXAMPLE 4 ----------

```
$singleSimpleTestSuiteTaskTarget = New-EnvTestDiscoveryTargetDefinition -TestSuiteId Infrastructure
$singleTestSuiteTaskTarget = New-EnvTestDiscoveryTargetDefinition -TestSuiteId Catalog -TargetIdType Catalog -TargetId $(Get-BrokerCatalog).Uuid
@($singleSimpleTestSuiteTaskTarget, $singleTestSuiteTaskTarget) | Start-EnvTestTask
```

Create two different discovery target definitions, put them in an array, then start a task based on both.

Remove-EnvTestServiceMetadata

Sep 10, 2014

Removes metadata from the given Service.

Syntax

```
Remove-EnvTestServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-EnvTestServiceMetadata [-ServiceHostId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-EnvTestServiceMetadata [-InputObject] <Service[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-EnvTestServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Service.

Related topics

Set-EnvTestServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-EnvTestService | % { Remove-EnvTestServiceMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Service objects.

Remove-EnvTestTask

Sep 10, 2014

Removes from the database completed tasks for the EnvTest Service.

Syntax

```
Remove-EnvTestTask [-TaskId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Remove-EnvTestTask [-Task <EnvTestTask>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables completed tasks that have run within the EnvTest Service to be removed from the database.

Related topics

Get-EnvTestDefinition

Get-EnvTestSuiteDefinition

Get-EnvTestTask

Start-EnvTestTask

Switch-EnvTestTask

Stop-EnvTestTask

Add-EnvTestTaskMetadata

Remove-EnvTestTaskMetadata

Parameters

-TaskId<Guid>

Specifies the identifier of the task to be removed, retrieveable from the $task.TaskId property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Task<EnvTestTask>

Specifies the task to be removed.

Required?	false

Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Examples

---------- EXAMPLE 1 ----------

```
Remove-EnvTestTask
```

Removes the current task from the EnvTest service.

---------- EXAMPLE 2 ----------

```
Remove-EnvTestTask -TaskId 50A4139F-2B55-4A97-A1BE-20EE4E124AA3
```

Removes a task from the EnvTest service via its id, which is available from an existing task's $task.TaskId property.

---------- EXAMPLE 3 ----------

```
$secondTask = $(Get-EnvTestTask -List)[1]
Remove-EnvTestTask -Task $secondTask
```

Removes the second task in the list returned by Get-EnvTestTask -List.

Remove-EnvTestTaskMetadata

Sep 10, 2014

Removes metadata from the given Task.

Syntax

```
Remove-EnvTestTaskMetadata [-TaskTaskId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-EnvTestTaskMetadata [-TaskTaskId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-EnvTestTaskMetadata [-InputObject] <EnvTestTask[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-EnvTestTaskMetadata [-InputObject] <EnvTestTask[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Task.

Related topics

Set-EnvTestTaskMetadata

Parameters

-TaskTaskId<Guid>

Id of the Task

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<EnvTestTask[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-EnvTestTask | % { Remove-EnvTestTaskMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Task objects.

Reset-EnvTestServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the EnvTest Service.

Syntax

```
Reset-EnvTestServiceGroupMembership [-ConfigServiceInstance] <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Enables you to reload EnvTest Service access permissions and configuration service locations. The Reset-EnvTestServiceGroupMembership command must be run on at least one instance of the service type (EnvTest) after installation and registration with the configuration service. Without this operation, the EnvTest services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-EnvTestServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Parameters

-ConfigServiceInstance<ServiceInstance[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.EnvTest.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-EnvTestServiceGroupMembership command.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-EnvTestServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-EnvTestServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Set-EnvTestConfiguration

Sep 10, 2014

Sets the Environment Test Service's configuation options

Syntax

Set-EnvTestConfiguration [-PerTypeDiscoveredObjectLimit <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Sets the Environment Test Service's configuation options and broadcasts the changes to other machines in the Site.

Related topics

Parameters

-PerTypeDiscoveredObjectLimit<Int32>

Sets the maximum number of objects of a particular type to be explored when discovering objects during a test run. Default: 50

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Integer Must be greater than zero.

Return Values

System.String

Examples

---------- EXAMPLE 1 ----------

```
Set-EnvTestConfiguration -PerTypeDiscoveredObjectLimit 100
```

Set the maximum to 100

Set-EnvTestDBConnection

Sep 10, 2014

Configures a database connection for the EnvTest Service.

Syntax

```
Set-EnvTestDBConnection [-DBConnection] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Configures a connection to a database in which the EnvTest Service can store its state. The service will attempt to connect and start using the database immediately after the connection is configured. The database connection string is updated to the specified value regardless of whether it is valid or not. Specifying an invalid connection string prevents a service from functioning until the error is corrected.

After a connection is configured, you cannot alter it without first clearing it (by setting the connection to $null).

You do not need to configure a database connection to use this command.

Related topics

Get-EnvTestServiceStatus

Get-EnvTestDBConnection

Test-EnvTestDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the EnvTest Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-EnvTestDBConnection command returns an object containing the status of the EnvTest Service together with extra diagnostics information.

DBUnconfigured

The EnvTest Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the EnvTest Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the EnvTest Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the EnvTest Service currently in use is incompatible with the version of the EnvTest Service schema on the database. Upgrade the EnvTest Service to a more recent version.

DBOlderVersionThanService

The version of the EnvTest Service schema on the database is incompatible with the version of the EnvTest Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The EnvTest Service is running and is connected to a database containing a valid schema.

Failed

The EnvTest Service has failed.

Unknown

The status of the EnvTest Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-EnvTestDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Configures a database connection string for the EnvTest Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Set-EnvTestDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Configures an invalid database connection string for the EnvTest Service.

Set-EnvTestServiceMetadata

Sep 10, 2014

Adds or updates metadata on the given Service.

Syntax

Set-EnvTestServiceMetadata [-ServiceHostId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-EnvTestServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-EnvTestServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-EnvTestServiceMetadata [-InputObject] <Service[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Allows you to store additional custom data against given Service objects.

Related topics

Remove-EnvTestServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Service specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true

Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-EnvTestServiceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

c:\PS>Set-EnvTestServiceMetadata -ServiceHostId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value


```
Key                             Value
---                             -----
property                        value
```

Add metadata with a name of 'property' and a value of 'value' to the Service with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-EnvTestTaskMetadata

Sep 10, 2014

Adds or updates metadata on the given Task.

Syntax

```
Set-EnvTestTaskMetadata [-TaskTaskId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-EnvTestTaskMetadata [-TaskTaskId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-EnvTestTaskMetadata [-InputObject] <EnvTestTask[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-EnvTestTaskMetadata [-InputObject] <EnvTestTask[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability for additional custom data to be stored against given Task objects.

Related topics

Remove-EnvTestTaskMetadata

Parameters

-TaskTaskId<Guid>

Id of the Task

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<EnvTestTask[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Task specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-EnvTestTaskMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-EnvTestTaskMetadata -TaskTaskId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                            -----
        property                           value
```

Add metadata with a name of 'property' and a value of 'value' to the Task with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Start-EnvTestTask

Sep 10, 2014

Starts a new test task.

Syntax

Start-EnvTestTask -TestId <String> [-TargetIdType <String>] [-TargetId <String>] [-CultureName <String>] [-IgnoreRelatedObjects] [-RunAsynchronously] [-ExcludeNotRunTests] [-AdminAddress <String>] [<CommonParameters>]

Start-EnvTestTask -TestSuiteId <String> [-TargetIdType <String>] [-TargetId <String>] [-CultureName <String>] [-IgnoreRelatedObjects] [-RunAsynchronously] [-ExcludeNotRunTests] [-AdminAddress <String>] [<CommonParameters>]

Start-EnvTestTask -InputObject <PSObject[]> [-CultureName <String>] [-IgnoreRelatedObjects] [-RunAsynchronously] [-ExcludeNotRunTests] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Starts a new test task based on a set of criteria provided via parameters or piped input and either waits for the tests to run or returns immediately depending on how it is called. When running a test suite and providing a target object for that suite, the service will discover related objects by default, but this behavior may be disabled if desired.

Related topics

Get-EnvTestDefinition

Get-EnvTestSuiteDefinition

Get-EnvTestTask

New-EnvTestDiscoveryTargetDefinition

Switch-EnvTestTask

Stop-EnvTestTask

Remove-EnvTestTask

Add-EnvTestTaskMetadata

Remove-EnvTestTaskMetadata

Parameters

-TestId<String>

Test identifiers. If specified, do not specify -TestSuiteId.

Required?	true
Default Value	Empty
Accept Pipeline Input?	false

-TestSuiteId<String>

Test suite identifiers. If specified, do not specify -TestId.

Required?	true
Default Value	Empty
Accept Pipeline Input?	false

-InputObject<PSObject[]>

One or more test targets defining the task, see Input Types for details about what kind of objects are permissible. Any valid object passed to this parameter may also be piped into this cmdlet.

Required?	true
Default Value	Empty
Accept Pipeline Input?	true (ByValue)

-TargetIdType<String>

Describes the type of corresponding object passed with -TargetId

Required?	false
Default Value	Empty
Accept Pipeline Input?	false

-TargetId<String>

The Ids that object tests or tests suites will target. By default, other components are queried for objects related to these.

Required?	false
Default Value	Empty
Accept Pipeline Input?	false

-CultureName<String>

The culture name in which to produce results. The culture name is in standard language/region-code format; for example "en-US".

Required?	false
Default Value	The current user interface culture
Accept Pipeline Input?	false

-IgnoreRelatedObjects<SwitchParameter>

Do not ask other components for objects related to a specified target.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-RunAsynchronously<SwitchParameter>

Do not wait for the test run to complete, return immediately.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-ExcludeNotRunTests<SwitchParameter>

If set, tests that are not run because no object matching their requirements is found are NOT included in test counts and results.

Required?	false
Default Value	False (include Not Run tests)
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.EnvTest.Sdk.EnvTestDiscoveryTargetDefinition A single EnvTestDiscoveryTargetDefinition can be specified to target one test or test suite. Citrix.EnvTest.Sdk.EnvTestDiscoveryTargetDefinition[] An array of EnvTestDiscoveryTargetDefinition(s) can be specified to target any combination of tests and/or test suites. PSCustomObject A single PSCustomObject with properties matching the required EnvTestDiscoveryTargetDefinition properties can be specified to target one test or test suite. PSCustomObject[] An array of PSCustomObject(s) with properties matching the required EnvTestDiscoveryTargetDefinition properties can be specified to target any combination of tests and/or test suites.

Return Values

Ctrix.EnvTest.Sdk.EnvTestTask

The newly started task.

Examples

---------- EXAMPLE 1 ----------

```
$singleSimpleTestTask = Start-EnvTestTask -TestId Monitor_RegisteredWithConfigurationService
```

Create and start a task with a single test and no target object.

---------- EXAMPLE 2 ----------

```
$singleSimpleTestTaskInSpanish = Start-EnvTestTask -TestId Monitor_RegisteredWithConfigurationService -CultureName es-ES
```

Create and start a task with a single test and no target object, with localized properties translated into Spanish.

---------- EXAMPLE 3 ----------

```
$singleSimpleTestSuiteTask = Start-EnvTestTask -TestSuiteId Infrastructure
```

Create and start a task with a single test suite and no target object.

---------- EXAMPLE 4 ----------

```
$singleTestSuiteTask = Start-EnvTestTask -TestSuiteId Catalog -TargetIdType Catalog -TargetId $(Get-BrokerCatalog).Uuid
```

Create and start a task with a single test suite and a catalog target object.

---------- EXAMPLE 5 ----------

```
$singleTestSuiteTask = Start-EnvTestTask -TestSuiteId Catalog -TargetIdType Catalog -TargetId $(Get-BrokerCatalog).Uuid -RunAsynchronously
```

Create and start a task with a single test suite and a catalog target object, and return immediately not waiting for the tests to complete.

---------- EXAMPLE 6 ----------

```
$adAccountPool = Get-AcctIdentityPool
    $singleTestTaskWithNoObjectDiscovery = StartEnvTestTask -IgnoreRelatedObjects -TestId ADIdentity_IdentityPool_ValidatePoolIsUnlocked -TargetIdType IdentityPo
```

Create and start a task with a single test, a target object for that test, and no object discovery based on that target.

---------- EXAMPLE 7 ----------

```
$singleSimpleTestSuiteTaskTarget = New-EnvTestDiscoveryTargetDefinition -TestSuiteId Infrastructure
    $singleTestSuiteTaskTarget = New-EnvTestDiscoveryTargetDefinition -TestSuiteId Catalog -TargetIdType Catalog -TargetId $(Get-BrokerCatalog).Uuid
    $inputObjects = @($singleSimpleTestSuiteTaskTarget, $singleTestSuiteTaskTarget)
    Start-EnvTestTask -InputObject $inputObjects
```

Create two different discovery target definitions, put them in an array, then start a task based on both via -InputObject.

Stop-EnvTestTask

Sep 10, 2014

Stops a still running task from completing.

Syntax

```
Stop-EnvTestTask [-TaskId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Stop-EnvTestTask [-Task <EnvTestTask>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Stops a still running task from completing. A task may still be retreived via Get-EnvTestTask until it Remove-EnvTestTask is called with its task id.

Related topics

Get-EnvTestDefinition

Get-EnvTestSuiteDefinition

Get-EnvTestTask

New-EnvTestTask

Start-EnvTestTask

Switch-EnvTestTask

Remove-EnvTestTask

Add-EnvTestTaskMetadata

Remove-EnvTestTaskMetadata

Parameters

-TaskId<Guid>

The id of the task to stop, retrieveable from the $task.TaskId property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Task<EnvTestTask>

An EnvTestTask representing the task to stop

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Examples

---------- EXAMPLE 1 ----------

```
Stop-EnvTestTask
```

Stops the current task from completing if it is still running.

---------- EXAMPLE 2 ----------

```
Stop-EnvTestTask -TestId 50A4139F-2B55-4A97-A1BE-20EE4E124AA3
```

Stops a task from completing via its id, which is available from an existing task's $task.TaskId property.

---------- EXAMPLE 3 ----------

```
$secondTask = $(Get-EnvTestTask -List)[1]
Stop-EnvTestTask -Task $secondTask
```

Stops the second task in the list returned by Get-EnvTestTask -List.

Switch-EnvTestTask

Sep 10, 2014

Sets the current task that will be returned by a call to Get-EnvTestTask with no parameters.

Syntax

```
Switch-EnvTestTask [-TaskId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

```
Switch-EnvTestTask [-Task <EnvTestTask>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Sets the current task that will be returned by a call to Get-EnvTestTask with no parameters.

Related topics

Get-EnvTestDefinition

Get-EnvTestSuiteDefinition

Get-EnvTestTask

New-EnvTestTask

Start-EnvTestTask

Stop-EnvTestTask

Remove-EnvTestTask

Add-EnvTestTaskMetadata

Remove-EnvTestTaskMetadata

Parameters

-TaskId<Guid>

Specifies the identifier of the task to be made current.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Task<EnvTestTask>

The task object to be made current, retrieveable from the $task.TaskId property.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.Management.Automation.PSObject Objects containing the TaskId parameter can be piped to the Remove-EnvTestTask command.

Examples

---------- EXAMPLE 1 ----------

```
Switch-EnvTestTask -TaskId 50A4139F-2B55-4A97-A1BE-20EE4E124AA3
```

Switches the current task to another via its id, which is available from an existing task's $task.TaskId property.

---------- EXAMPLE 2 ----------

```
$secondTask = $(Get-EnvTestTask -List)[1]
Switch-EnvTestTask -Task $switchTask
```

Switches the current task to the second in the list returned by Get-EnvTestTask -List.

Test-EnvTestDBConnection

Sep 10, 2014

Tests a database connection for the EnvTest Service.

Syntax

```
Test-EnvTestDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Tests a connection to the database in which the EnvTest Service can store its state. The service will attempt to connect to the database without affecting the current connection to the database.

You do not have to clear the connection to use this command.

Related topics

Get-EnvTestServiceStatus

Get-EnvTestDBConnection

Set-EnvTestDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the EnvTest Service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-EnvTestDBConnection command returns an object containing the status of the EnvTest Service if the connection string of the specified data store were to be set to the string being tested, together with extra diagnostics information for the specified connection string.

DBRejectedConnection

The database rejected the logon attempt from the EnvTest Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the EnvTest Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the EnvTest Service currently in use is incompatible with the version of the EnvTest Service schema on the database. Upgrade the EnvTest Service to a more recent version.

DBOlderVersionThanService

The version of the EnvTest Service schema on the database is incompatible with the version of the EnvTest Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Set-EnvTestDBConnection command would succeed if it were executed with the supplied connection string.

Failed

The EnvTest Service has failed.

Unknown

The status of the EnvTest Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Test-EnvTestDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"
```

OK
Tests a database connection string for the EnvTest Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Test-EnvTestDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Tests an invalid database connection string for the EnvTest Service.

Citrix.Host.Admin.V2

Sep 10, 2014

Overview

Name	Description
HypHostSnapin	The Host Service PowerShell snap-in provides administrative functions for
Hyp Filtering	Describes the common filtering options for XenDesktop cmdlets.

Cmdlets

Name	Description
Add-HypHostingUnitMetadata	Adds metadata on the given HostingUnit.
Add-HypHostingUnitNetwork	Makes additional hypervisor networks available for use in a HostingUnit.
Add-HypHostingUnitStorage	Adds storage locations to a hosting unit.
Add-HypHypervisorConnectionAddress	Add a connection address to a hypervisor connection.
Add-HypHypervisorConnectionMetadata	Adds metadata on the given HypervisorConnection.
Add-HypHypervisorConnectionScope	Add the specified HypervisorConnection(s) to the given scope(s).
Add-HypMetadata	Adds metadata to a hypervisor connection or a hosting unit.
Get-HypConfigurationDataForItem	Retrieves the configuration data for an item in the Host Service provider path. Note: For this release, only VM items are supported for this operation.
Get-HypConfigurationObjectForItem	Retrieves the configuration data for an item in the Host Service provider path. Note: For this release, only VM items are supported for this operation.
Get-HypConnectionRegion	Enumerates the regions of a hypervisor connection that are based on cloud technology.
Get-HypDBConnection	Gets the database string for the specified data store used by the Host Service.

Name	Description
Get-HypDBSchema	Gets a script that creates the Host Service database schema for the specified data store.
Get-HypDBVersionChangeScript	Gets a script that updates the Host Service database schema.
Get-HypHypervisorPlugin	Gets the available hypervisor types.
Get-HypInstalledDBVersion	Gets a list of all available database schema versions for the Host Service.
Get-HypScopedObject	Gets the details of the scoped objects for the Host Service.
Get-HypService	Gets the service record entries for the Host Service.
Get-HypServiceAddedCapability	Gets any added capabilities for the Host Service on the controller.
Get-HypServiceInstance	Gets the service instance entries for the Host Service.
Get-HypServiceStatus	Gets the current status of the Host Service on the controller.
Get-HypVMMacAddress	Retrieves a list the MAC addresses for the VMs in the specified connection.
Get-HypVolumeServiceConfiguration	Gets instances of the VolumeServiceConfiguration that are configured for this site.
Get-HypXenServerAddress	Gets all the available addresses for a XenServer hypervisor connection.
Grant-HypSecurityGroupEgress	Adds an egress rule to a security group.
Grant-HypSecurityGroupIngress	Adds an ingress rule to a security group.
New-HypVMSnapshot	Creates a new snapshot for the specified VM item path.
Remove-HypHostingUnitMetadata	Removes metadata from the given HostingUnit.
Remove-HypHostingUnitNetwork	Removes networks from a hosting unit.
Remove-HypHostingUnitStorage	Removes storage from a hosting unit.
Remove-HypHypervisorConnectionAddress	Removes addresses from the list of available connection addresses.

Name	Description
Remove-HypHypervisorConnectionMetadata	Removes metadata from the given HypervisorConnection.
Remove-HypHypervisorConnectionScope	Remove the specified HypervisorConnection(s) from the given scope(s).
Remove-HypMetadata	Removes metadata from a hypervisor connection or hosting unit.
Remove-HypServiceMetadata	Removes metadata from the given Service.
Reset-HypServiceGroupMembership	Reloads the access permissions and configuration service locations for the Host Service.
Revoke-HypSecurityGroupEgress	Removes an egress rule from a security group.
Revoke-HypSecurityGroupIngress	Removes an ingress rule from a security group.
Set-HypAdminConnection	Set the controller to be used by the cmdlets that form the Host service PowerShell snap-in.
Set-HypDBConnection	Configures a database connection for the Host Service.
Set-HypHostingUnitMetadata	Adds or updates metadata on the given HostingUnit.
Set-HypHostingUnitStorage	Sets options for a storage location on a hosting unit.
Set-HypHypervisorConnectionMetadata	Adds or updates metadata on the given HypervisorConnection.
Set-HypServiceMetadata	Adds or updates metadata on the given Service.
Set-HypVolumeServiceConfiguration	Applies a change to one of the VolumeServiceConfiguration instances in the site.
Start-HypVM	Starts a VM.
Stop-HypVM	Stops a VM by issuing a Shutdown request
Test-HypDBConnection	Tests a database connection for the Host Service.
Test-HypHostingUnitNameAvailable	Checks to ensure that the proposed name for a hosting unit is unused.

Name	Description
Test-HypHypervisorConnectionNameAvailable	Checks to ensure that the proposed name for a hypervisor connection is unused.
Update-HypHypervisorConnection	Requests the host service to update the connection properties that depend on the version of hypervisor in use.

about_HypHostSnapin

Sep 10, 2014

TOPIC

about_HypHostSnapin

SHORT DESCRIPTION

The Host Service PowerShell snap-in provides administrative functions for the Host Service.

COMMAND PREFIX

All commands in this snap-in have 'Hyp' in their name.

LONG DESCRIPTION

The Host Service PowerShell snap-in enables both local and remote administration of the Host Service. It lets you configure XenDesktop deployments to make use of hypervisors, networks, and storage, and enables browsing of their contents using the Host PowerShell provider (Citrix.HypervisorProvider).

The provider creates a default PSDrive with a drive identifier of 'XDHyp'. This drive provides two root folders:

HostingUnits Folder

> Contains a list of all the hosting units that have been defined using the new-Item provider command.
>
> Hosting units define not only a hypervisor connection, but also reference networks and storage. Hosting units are used by the Machine Creation Service to provide the information required to create and manage virtual machines that can be used by other services. A hosting unit references a root path. This is a specific point in the provider connection tree. The hosting unit is constrained to provide only items below this point in the tree. This restricts the locations that the Machine Creation Service can use to create virtual machines and the networks and storage that can be used.

Connections Folder

> Contains a list of all the hosting unit connections that are defined using the new-Item provider command.
>
> Change directory to a specific connection and use the dir/Get-ChildItem command to list all of the infrastructure (such as folders, hypervisors, networks, storage, and virtual machines) that is available in the hosting unit to which the connection refers. The paths to these items

are used as the input to commands in the Host Service and Machine Creation Service snap-ins.

The contents of the Hosting Unit and Connection folders reflect the content and structure of the hypervisor to which they refer. The item extensions reflect the object type for each item. Not all item types are appropriate for all hypervisor types. Possible item types are:

Virtual Machine (.vm)
Snapshot (.snapshot)
Cluster (.cluster)
Host (.host)
HostGroup (.hostgroup)
DataCenter (.datacenter)
Folder (.folder)
ResourcePool (.resourcepool)
ComputeResource (.computeresource)

When used with a path that refers to the Host provider (with a default drive of 'XDHyp:'), the Host provider extends the standard New-Item, Get-Item, Get-ChildItem, Remove-Item, Rename-Item, and Set-Item commands as described below. For more information about the basic behavior of these commands, see the help for the command. The Move-Item and Copy-Item commands are not supported for the Host provider.

New-Item

The following parameters are available when using New-Item in the Connections directory (or a path that refers to the directory). The Credential parameter is not supported.

-Name
Specifies the name of the connection, which must not contain any of the following characters: \/;:#.*?=<>|[]()"'{}. The Name parameter is optional but, if not included, the connection name must be specified as part of the Path parameter.

-HypervisorAddress <String[]>
Specifies an array of addresses that can be used to contact the required hypervisor. All the addresses are considered equivalent, that is, all of the addresses provide access to the same virtual machines, snapshots, network, and storage.

-ConnectionType <ConnectionType>
Specifies the type of hypervisor that the connection is for. Supported hypervisor types are:

XenServer

SCVMM (Microsoft Hyper-V)
vCenter (VMware vSphere/ESX)
Custom

-PluginId <String>
Specifies the class name for the Citrix Managed Machine library that is used to access the hypervisor. You can obtain this list using the Get-HypHypervisorPlugin command. The PluginId parameter must be specified if the ConnectionType is set to 'Custom'.

-UserName <String>, -Password <String>, -SecurePassword <SecureString>
Specifies the credentials for the connection to the hypervisor. You can specify the password as either Password or SecurePassword, but not both. The UserName parameter, and either Password or SecurePassword, specify the same information as the HypervisorCredential parameter, so use of one precludes use of the other.

-HypervisorCredential <PSCredential>
Specifies credentials for the connection to the hypervisor. The HypervisorCredential parameter specifies the same information as UserName and either Password or SecurePassword, so use of one precludes use of the other.

-Persist
Specifies that the connection details are persistent. If this parameter is not included, the connection is held only for the duration of the current runspace and PSDrive combination. Only persistent connection items are visible to administrators in other runspaces and PSDrives. Hosting units cannot be created from connections that are not persistent.

-AdminAddress <String>
Specifies the address of the Host Service that the command communicates with. After it is set, this address is used for all commands in the Host Service PowerShell snap-in. If this parameter is not included or set by another command, or if Set-HypAdminConnection has not been used, the command attempts to use a local Host Service.

-LoggingId <String>
Specifies the identifier of the high-level operation that this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

-Scopes <String[]>

Specifies the list of administrative scopes that the new connection will be a part of. The scopes control which administrators are able to work with the connection.

The following parameters are available when using New-Item in the HostingUnits directory (or a path that refers to the directory).

-Name
Specifies the name of the hosting unit, which must not contain any of the following characters: \/;:#.*?=<>|[]()"'{}. The Name parameter is optional but, if not included, the hosting unit name must be provided as part of the Path parameter.

-HypervisorConnectionName <String>
Specifies the name of the connection that the hosting unit uses. To create a hosting unit, the referenced connection must be persistent and the ConnectionType must not be set to 'Custom'.

-HypervisorConnectionUid <Guid>
Specifies the unique identifier of the connection that the hosting unit uses. To create a hosting unit, the referenced connection must be persistent and the ConnectionType must not be set to 'Custom'.

-RootPath <String>
Specifies the location in a connection that is used as the starting reference for the hosting unit. The path must point to an item in the connection that is marked as a SymLink. The root of a XenServer connection is a special case that is also considered a SymLink. If this parameter is not included, the current location in the provider is used.

-NetworkPath <String>
Specifies the path in a connection to the network item that is used when the Machine Creation Service creates new virtual machines.

-StoragePath <String>
Specifies one or more paths in a connection to storage items that are used when the Machine Creation Service creates new virtual machines. After they are set, you can modify storage paths using the Add-HypHostingUnitStorage and Remove-HypHostingUnitStorage commands. If the connection is based on cloud infrastructure, storage items are typically not available, in which case this parameter can be omitted.

-PersonalvDiskStoragePath <String>
Specifies one or more paths in a connection to storage items

that are used when the Machine Creation Service creates disks
for the virtual machines. After they are set, you can modify storage paths
using the Add-HypHostingUnitStorage and Remove-HypHostingUnitStorage
commands.

-NoVmTagging
Specifies that new virtual machines are not tagged with
metadata from the hypervisor. By default, all virtual machines
created by the Machine Creation Service are tagged to show they are created
by XenDesktop. These tags are used by the provider to restrict the
list of virtual machines displayed when viewing the content of the
Connections or HostingUnit paths. If this parameter is not
included, all virtual machines are displayed at all times.

-AdminAddress <String>
Specifies the address of the Host Service that the command will
communicate with. After it is set, this address is used for all commands
in the Host Service PowerShell snap-in. If this parameter is not
included or set by another command, or if Set-HypAdminConnection
has not been used, the command attempts to use a local Host
Service.

-UseLocalStorageCaching
When Get-HypServiceAddedCapability indicates that the LocalStorageCaching
feature is available, use this parameter to specify that
the virtual machines created for this hosting unit will use local
storage caching for their disk images.

-GpuGroup

Specifies a path to a GPU Group in a connection that will be used when

Machine Creation Services creates VMs. Only a single GPU Group is supported and the value is immutable.

-LoggingId <String>
Specifies the identifier of the high-level operation that this cmdlet call
forms a part of. Citrix Studio and Director typically create
high-level operations. PowerShell scripts can also wrap a series of cmdlet
calls in a high-level operation by way of the Start-LogHighLevelOperation
and Stop-LogHighLevelOperation cmdlets.

The following parameters are available when using New-Item relative to a
connection or hosting unit.

-ItemType <string>
Specifies the type of item to create when invoked relative to a connection
or hosting unit. Supported ItemType values are:

SecurityGroup (cloud only)

-Description
Specifies a description for the security group.

-VpcId
Specifies a VPC ID for the security group.

Get-Item

Get-ChildItem (alias dir)

Rename-Item

Remove-Item

The following additional parameters are available.

AdminAddress
Specifies the address of the Host Service that the command communicates with. After it is set, this address is used for all commands in the Host Service PowerShell snap-in. If this parameter is not included or set by another command, or if Set-HypAdminConnection has not been used, the command attempts to use a local Host Service.

-LoggingId <String>
Specifies the identifier of the high-level operation that this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

You can specify the Path parameter by name or by using the unique identifier for the connection or hosting unit enclosed in braces. For example:

-Path XDHyp:\{1233-3213ACDF-12323}

The Filter parameter is not supported. Virtual machines created by the Machine Creation Service are returned only if the -Force parameter is used or if virtual machine tagging was disabled on the hosting unit with the NoVmTagging parameter when the VMs were created.

The following parameters are available when using Set-Item in the Connections directory.

-UserName <String>, -Password <String>, -SecurePassword <SecureString>
Specifies the credentials for the connection to the hypervisor. The password can be given as either Password or SecurePassword, but not both. The UserName parameter and either Password or SecurePassword specify the same information as the HypervisorCredential parameter, so use of one precludes use of the other.

-HypervisorCredential <PSCredential>
Specifies credentials for the connection to the hypervisor. The HypervisorCredential parameter specifies the same information as the UserName parameter and either Password or SecurePassword, so use of one precludes use of the other.

-HypervisorAddress <string[]>
Specifies the addresses of the hypervisor that this connection represents. This replaces all existing addresses.

-LoggingId <String>
Specifies the identifier of the high-level operation that this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

-MaintenanceMode <Boolean>
Places the connection into maintenance mode which disables all communication between XenDesktop and the Hypervisor. Use this mode when making changes to the hypervisor; for instance, if the password for the access account needs to be changed.

-AdminAddress <String>
Specifies the address of the Host Service that the command communicates with. After it is set, this address is used for all commands in the Host Service PowerShell snap-in. If this parameter is not included or set by another command, or if Set-HypAdminConnection has not been used, the command tries to use a local Host Service.

The Credential parameter is not supported. Addresses can be modified with the Add-HypHypervisorConnectionAddress and Remove-HypHypervisorConnectionAddress commands. Metadata can be modified with the Add-HypMetadata and Remove-HypMetadata commands.

The following parameters are available when using New-Item in the

HostingUnits directory.

-Name
    Specifies the name of the hosting unit, which must not contain any
    of the following characters: \/;:#.*?=<>|[]()"'{}. The Name
    parameter is optional but, if not included, the hosting unit name
    must be provided as part of the Path parameter.

-NetworkPath <String>
    Specifies the path in a connection to the network item that
    is used when the Machine Creation Service creates new virtual
    machines.

-NoVmTagging
    Specifies that new virtual machines are not tagged with
    metadata from the hypervisor. By default, all virtual machines
    created by the Machine Creation Service are tagged to show they are created
    by XenDesktop. These tags are used by the provider to restrict the
    list of virtual machines displayed when viewing the content of the
    Connections or HostingUnit paths. If this parameter is not
    included, all virtual machines are displayed at all times.

-AdminAddress <String>
    Specifies the address of the Host Service that the command
    communicates with. After it is set, this address is used for all commands
    in the Host Service PowerShell snap-in. If this parameter is not
    included or set by another command, or if Set-HypAdminConnection
    has not been used, the command attempts to use a local Host
    Service.

-UseLocalStorageCaching <bool>
    When Get-HypServiceAddedCapability indicates that the LocalStorageCaching
    feature is available, use this parameter to specify that
    the virtual machines created for this hosting unit will use local
    storage caching for their disk images.

-LoggingId <String>
    Specifies the identifier of the high-level operation that this cmdlet call
    forms a part of. Citrix Studio and Director typically create
    high-level operations. PowerShell scripts can also wrap a series of cmdlet
    calls in a high-level operation by way of the Start-LogHighLevelOperation
    and Stop-LogHighLevelOperation cmdlets.

Storage can be modified with the Add-HypHostingUnitStorage and
Remove-HypHostingUnitStorage commands. Metadata can be modified with
the Add-HypMetadata and Remove-HypMetadata commands.

The item types returned when these commands are used in the Host Service provider are defined in the Object Definitions section below.

EXAMPLES

To Create a Persistent Hypervisor Connection

```
new-item -path "xdhyp:\Connections" -Name MyConn -ConnectionType
   XenServer -HypervisorAddress "http:\\address" -UserName user
   -Password password -Persist

PSPath:                Citrix.HostingUnitService.Admin.V1.0\
                       Citrix.Hypervisor::XDHyp:\Connections\MyConn
PSParentPath:          Citrix.HostingUnitService.Admin.V1.0\
                       Citrix.Hypervisor::XDHyp:\Connections
PSChildName:           MyConn
PSDrive:               XDHyp
PSProvider:            Citrix.HostingUnitService.Admin.V1.0\
                       Citrix.Hypervisor
PSIsContainer:         True
HypervisorConnectionUid:  04e6daa2-5cbd-4491-b70c-6daf733ee82a
HypervisorConnectionName: MyConn
ConnectionType:        XenServer
HypervisorAddress:     {http:\\address}
UserName:              user
Persistent:            True
PluginId:              XenFactory
SupportsPvsVMs:        True
Revision:              1b0b0d02-bc1b-49d8-b2b0-be6fb7f150ad
MaintenanceMode:       False
Metadata:              {MaxAbsoluteActiveActions = 100,
                       MaxAbsoluteNewActionsPerMinute = 100,
                       MaxPowerActionsPercentageOfDesktops = 20}
```

To Create a Hosting Unit

```
new-item -Path "xdhyp:\HostingUnits"
   -Name MyHU
   -HypervisorConnectionName MyConn
   -RootPath XDHYP:\Connections\MyConn
   -NetworkPath XDHYP:\Connections\MyConn\Network 0.network
   -StoragePath XDHYP:\Connections\MyConn\Local storage on
   myXenServer.storage

PSPath:              Citrix.HostingUnitService.Admin.V1.0\
                     Citrix.Hypervisor::XDHyp:\HostingUnits\MyHU
PSParentPath:        Citrix.HostingUnitService.Admin.V1.0\
                     Citrix.Hypervisor::XDHyp:\HostingUnits
```

```
PSChildName:         MyHU
PSDrive:             XDHyp
PSProvider:          Citrix.HostingUnitService.Admin.V1.0\
                   Citrix.Hypervisor
PSIsContainer:       True
HostingUnitUid:      df91f886-1141-4280-bd59-2ee260a4df79
HostingUnitName:     MyHU
HypervisorConnection: MyConn
RootPath:            /
RootId:
NetworkPath:         /Network 0.network
NetworkId:           ab47080b-ca15-771a-c8dc-6ad9650158f1
Storage:             {/Local storage on myXenServer.storage}
VMTaggingEnabled:    True
Metadata:            {}
```

Relative paths can be used for all parameters.

OBJECT DEFINITIONS

Citrix.XDInterServiceTypes.HypervisorConnection

The hypervisor connection object is returned when a connection item is located. This item has the following parameters.

HypervisorConnectionUid <Guid>
Specifies the unique identifier for the connection item.

HypervisorConnectionName <String>
Specifies the name of the connection item.

ConnectionType <Citrix.XDInterServiceTypes.ConnectionType>
Specifies the type of hypervisor that the connection is for.
Supported hypervisor types are:

- XenServer
- SCVMM (Microsoft Hyper-V)
- vCenter (VMware vSphere/ESX)
- Custom

HypervisorAddress <String[]>
Specifies the addresses that can be used to contact the required hypervisor.

Username <String>
Specifies the administrator user name for the connection to the hypervisor (from the user name and password given as administrator credentials when

setting up this connection)

Persistent <Boolean>
Specifies whether or not the connection is persistent.

PluginId <String>
Specifies the Citrix Managed Machine class identifier for the hypervisor.

SupportsPvsVM <Boolean>
Specifies whether or not the connection can be used as part of a hosting unit. If this parameter is set to 'True', a hosting unit referencing this connection can be created.

Revision <Guid>
A unique identifier that is changed every time any properties of the connection are changed.

MaintenanceMode <Boolean>
Specifies whether or not the connection is currently in maintenance mode.

Metadata <Citrix.XDInterServiceTypes.Metadata[]>
The collection of metadata associated with the connection.

Citrix.XDInterServiceTypes.HostingUnit

The hosting unit object is returned when a hosting unit item is located. This item has the following parameters.

HostingUnitName <String>
Specifies the name of the hosting unit.

HostingUnitUid <Guid>
Specifies the unique identifier for the hosting unit.

HypervisorConnection <Citrix.XDInterServiceTypes.HypervisorConnection>
Specifies the hypervisor connection item that the hosting unit references.

NetworkId <String>
Specifies the unique identifier for the network in the hypervisor context that the hosting unit references.

NetworkPath <String>
Specifies the path to the network in the Host Service provider.

RootId <String>
Specifies the unique identifier for the root connection item in the hypervisor context that the hosting unit references.

RootPath <String>
Specifies the path to the root of the hosting unit from within the Host Service provider.

Storage <Citrix.XDInterServiceTypes.Storage[]>
Specifies the collection of storage objects that are defined for use as part of the hosting unit. This object contains the following parameters.

StorageID <String>
Specifies the identifier for the storage in the hypervisor context.

StoragePath <String>
Specifies the path to the storage in the Host Service provider.

VMTaggingEnabled <Boolean>
Specifies whether or not virtual machine metadata is used to tag virtual machines created by XenDesktop.

Metadata <Citrix.XDInterServiceTypes.Metadata[]>
Specifies the collection of metadata associated with the hosting unit.

Citrix.HostingUnitService.Sdk.HypervisorObject

The hypervisor object is returned when any item is located from within a Connection or HostingUnit folder. This item has the following parameters.

AdditionalData <Dictionary<String,String>
Stores extra untyped data for the item. This dictionary contains different information for each item type.

For Storage Items
Key = StorageType
Values = Shared or Local

For VM Items

Key = PowerState Values = PoweredOn,

PoweredOff,

Suspended,
TransitioningToOn,
TransitioningToOff,
Suspending,
Resuming,
Unknown,
Error

Name <String>
Specifies the name of the item.

FullName <String>
Specifies the name with the appropriate file extension.

ObjectPath <String>
Specifies the relative path to the item from the root of the connection of which the item is part.

FullPath <String>
Specifies the absolute path to the item in the Citrix.Hypervisor provider.

Id <String>
Specifies the identity of the item in the hypervisor context.

IsContainer <Boolean>
Specifies whether or not the item can contain other items.

IsSymLink <Boolean>
Specifies whether or not the item can be used as a RootPath of a hosting unit.

ObjectType <Citrix.HostingUnitService.Sdk.NodeType>
Specifies the item type.

ERROR CODES

The provider commands can return the following error codes.

New-Item

ConnectionNameOrUidInvalid
The name or unique identifier of the hypervisor connection

specified for the hosting unit is invalid.

HostingUnitRootPathInvalid
The root path specified for the hosting unit is invalid. The root path must be a valid item in the hypervisor tree and a SymLink.

HostingUnitNetworkPathInvalid
The network path specified for the hosting unit is invalid. The network path must be a valid item in the hypervisor tree and relative to the root path.

HostingUnitStoragePathInvalid
The storage path specified for the hosting unit is invalid. The storage path must be a valid item in the hypervisor tree and relative to the root path.

HostingUnitDuplicateObjectExists
A hosting unit object with the same name already exists. Hosting unit names must be unique.

HostingUnitStorageDuplicateObjectExists
A hosting unit storage object with the same storage path already exists for this hosting unit. There can be only one object for each combination of hosting unit and storage path.

HypervisorNotContactable
The hypervisor could not be contacted at the supplied address, which is either invalid or unreachable.

HypervisorAddressInvalidFormat
The address is not in a valid form for the specified hypervisor type.

ConnectionAddressInvalid
The specified address is invalid and does not belong to the same pool.

HypervisorConnectionDuplicateObjectExists
A hypervisor connection object with the same name already exists. Hypervisor connection names must be unique.

HypervisorConnectionAddressDuplicateObjectExists
A hypervisor connection address object with the same address already exists for this hypervisor connection. There can be only one object for each combination of hypervisor connection and address.

HypervisorConnectionForHostingUnitIsVirtual
The specified hypervisor connection for the hosting unit is a virtual

non-persistent connection. A persistent connection is required when creating a hosting unit.

InputNameInvalid
The name specified for the hosting unit or hypervisor connection is invalid because it contains one or more of the following characters: \/;:#.*?=<>|[]()"'{}.

InputPathInvalid
The specified path is invalid because it is not in one of the following formats:

XDHyp:\Connections\<Name>
XDHyp:\Connections\{Guid}

ExceptionThrown
An unexpected error occurred.

DatabaseError
There was a problem communicating with the database.

CommunicationError
There was a problem communicating with the remote service.

PermissionDenied
The user does not have administrative rights to perform this operation.

ScopeNotFound
One or more of the scopes nominated for the new connection do not exist.

CannotCreateSecurityGroupHere
Security groups can only be created in a virtual private cloud (VPC).

Get-Item and Get-ChildItem

HypervisorConnectionObjectNotFound
The hypervisor connection object specified in the path could not be found.

HostingUnitObjectNotFound
The specified hosting unit object could not be found.

HypervisorInMaintenanceMode

The hypervisor for the specified connection is currently in maintenance mode and cannot be accessed.

FailureToRetrieveConnectionPassword
The password for the HypervisorConnection cannot be retrieved or decrypted.

ExceptionThrown
An unexpected error occurred.

DatabaseError
There was a problem communicating with the database.

CommunicationError
There was a problem communicating with the remote service.

Remove-Item

HostingUnitObjectToDeleteDoesNotExist
The specified hosting unit object does not exist.

HypervisorConnectionObjectToDeleteDoesNotExist
The specified hypervisor connection object does not exist.

InputPathInvalid
The specified path is invalid because it is not in one of the following formats:

XDHyp:\Connections\<Name>
XDHyp:\Connections\{Guid}
XDHyp:\HostingUnits\<Name>
XDHyp:\HostingUnits\{Guid}

HypervisorConnectionObjectToDeleteIsInUse
The specified hypervisor connection object cannot be deleted because it is being used by one or more hosting units.

ExceptionThrown
An unexpected error occurred.

DatabaseError
There was a problem communicating with the database.

CommunicationError
There was a problem communicating with the remote service.

ObjectCannotBeRemoved
The specified object cannot be removed.

Rename-Item

InputPathInvalid
The specified path is invalid because it is not in one of the following formats:

XDHyp:\Connections\<Name>
XDHyp:\Connections\{Guid}
XDHyp:\HostingUnits\<Name>
XDHyp:\HostingUnits\{Guid}

HostingUnitDuplicateNameExists
A hosting unit object with the same name already exists. Hosting unit names must be unique.

HypervisorConnectionDuplicateNameExists
A hypervisor connection object with the same name already exists. Hypervisor connection names must be unique.

InputNameInvalid
The new name specified for the hosting unit or hypervisor connection is invalid because it contains one or more of the following characters: \/;:#.*?=<>|[]()"'{}.

ExceptionThrown
An unexpected error occurred.

DatabaseError
There was a problem communicating with the database.

CommunicationError
There was a problem communicating with the remote service.

Set-Item

InputPathInvalid
The specified path is invalid because it is not in one of the following formats:

XDHyp:\Connections\<Name>
XDHyp:\Connections\{Guid}
XDHyp:\HostingUnits\<Name>
XDHyp:\HostingUnits\{Guid}

HostingUnitObjectToUpdateDoesNotExist
The specified hosting unit object does not exist.

HostingUnitNetworkPathInvalid
The new network path specified for the hosting unit is invalid. Either the network path does not exist or it is not relative to the root path of the hosting unit.

HypervisorConnectionObjectToUpdateDoesNotExist
The specified hypervisor connection object does not exist.

ExceptionThrown
An unexpected error occurred.

DatabaseError
There was a problem communicating with the database.

DatabaseNotConfigured
The operation could not be completed because the database for the service is not configured.

DataStoreException
An error occurred in the service while attempting a database operation. Communication with the database failed for various reasons.

CommunicationError
There was a problem communicating with the remote service.

about_Hyp_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```

retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

```
A120901
B220000
...
```

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

Add-HypHostingUnitMetadata

Sep 10, 2014

Adds metadata on the given HostingUnit.

Syntax

Add-HypHostingUnitMetadata [-HostingUnitUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHostingUnitMetadata [-HostingUnitUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHostingUnitMetadata [-HostingUnitName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHostingUnitMetadata [-HostingUnitName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHostingUnitMetadata [-InputObject] <HostingUnit[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHostingUnitMetadata [-InputObject] <HostingUnit[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given HostingUnit objects. This cmdlet will not overwrite existing metadata on an object - use the Set-HypHostingUnitMetadata cmdlet instead.

Related topics

Set-HypHostingUnitMetadata

Remove-HypHostingUnitMetadata

Parameters

-HostingUnitUid<Guid>

Id of the HostingUnit

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HostingUnitName<String>

Name of the HostingUnit

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<HostingUnit[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the HostingUnit specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Host.Sdk.Metadata

Add-HypHostingUnitMetadata returns an array of objects containing the new definition of the metadata.

\n Property <string>

\n Specifies the name of the property.

\n Value <string>

\n Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DuplicateObject

One of the specified metadata already exists.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-HypHostingUnitMetadata -HostingUnitUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Property                       Value
        --------                      -----
        property                       value
```

Add metadata with a name of 'property' and a value of 'value' to the HostingUnit with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Add-HypHostingUnitNetwork

Sep 10, 2014

Makes additional hypervisor networks available for use in a HostingUnit.

Syntax

```
Add-HypHostingUnitNetwork [-LiteralPath] <String> [-NetworkPath] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to extend the set of hypervisor networks that are made available through the HostingUnit to the Citrix Machine Creation Service. When new machines are created, their virtual NICs can be associated only with networks that are in this set. This command cannot be used if the connection for the hosting unit is in maintenance mode.

Related topics

New-Item

Add-HypMetadata

remove-HypHostingUnitNetwork

Parameters

-LiteralPath<String>

Specifies the path to the hosting unit to which the network will be added. The path must be in one of the following formats: <drive>:\HostingUnits\<HostingUnitName> or <drive>:\HostingUnits\{<HostingUnit Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	false

-NetworkPath<String>

Specifies the path to the network that will be added. The path must be in one of the following formats: <drive>:\Connections\<ConnectionName>\MyNetwork.network or <drive>:\Connections\{<Connection Uid>}\MyNetwork.network or <drive>:\HostingUnits\<HostingUnitName>\MyNetwork.network or <drive>:\HostingUnits\{<hostingUnit Uid>}\MyNetwork.network

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. This can be a host name or an IP address.

Required?	false
Default Value	LocalHost. When a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Add-HypHostingUnitNetwork (NetworkPath parameter).

Return Values

Citrix.Host.Sdk.HostingUnit

Add-HypHostingUnitNetwork returns an object containing the new definition of the hosting unit.

HostingUnitUid <Guid>

Specifies the unique identifier for the hosting unit.

HostingUnitName <string>

Specifies the name of the hosting unit.

HypervisorConnection <Citrix.Host.Sdk.HypervisorConnection>

Specifies the connection that the hosting unit uses to access a hypervisor.

RootId <string>

Identifies, to the hypervisor, the root of the hosting unit.

RootPath <string>

The hosting unit provider path that represents the root of the hosting unit.

Storage <Citrix.Host.Sdk.Storage[]>

The list of storage items that the hosting unit can use.

PersonalvDiskStorage <Citrix.XDPowerShell.Storage[]>

The list of storage items that the hosting unit can use for storing personal data.

VMTaggingEnabled <Boolean>

Specifies whether or not the metadata in the hypervisor can be used to store information about the XenDesktop Machine Creation Service.

NetworkId <string>

The hypervisor's internal identifier that represents the default network specified for the hosting unit.

NetworkPath <string>

The hosting unit provider path to the default network specified for the hosting unit.

Metadata <Citrix.Host.Sdk.Metadata[]>

A list of key value pairs that can store additional information about the hosting unit.

PermittedNetworks <Citrix.Host.Sdk.Network[]>

A full list of the hypervisor networks that are exposed for use in the hosting unit.

Notes

The network path must be valid for the hosting unit. The rules that are applied are as follows: XenServer (HypervisorConnection Type = XenServer)

NA

VMWare vSphere/ESX (HypervisorConnection Type = vCenter)

The network path must be directly contained in the root path item of the hosting unit.

Microsoft SCVMM/Hyper-v (HypervisorConnection Type = SCVMM)

NA

In the case of failure, the following errors can result.

Error Codes

HostingUnitsPathInvalid

The path provided is not to an item in a subdirectory of a hosting unit item.

HostingUnitNetworkPathInvalid

The specified path is invalid.

HostingUnitNetworkPathInvalid

The network path cannot be found or is invalid. See notes above about validity.

HostingUnitNetworkDuplicateObjectExists

The specified network path is already part of the hosting unit.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation. Communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-HypHostingUnitNetwork -LiteralPath XDHyp:\HostingUnits\MyHostingUnit -NetworkPath 'XDHyp:\HostingUnits\MyHostingUnits\newNetwork.network'

        HostingUnitUid      : bcd3d649-86d1-4aa8-8ec2-d322b6a2c457
        HostingUnitName     : MyHostingUnit
        HypervisorConnection : MyConnection
        RootPath            : /
        RootId              :
        NetworkPath         : /Network 0.network
        NetworkId           : ab47080b-ca15-771a-c8dc-6ad9650158f1
        Storage             : {/Local storage.storage}
        PersonalvDiskStorage : {}
        VMTaggingEnabled    : True
        Metadata            : {}
        PermittedNetworks   : {/Network 0.network, /newNetwork.network}
```

The command adds a new network called "newNetwork.network" to the hosting unit called "MyHostingUnit".

---------- EXAMPLE 2 ----------

```
XDHyp:\HostingUnits\MyHostingUnit>Add-HypHostingUnitNetwork -LiteralPath . -NetworkPath 'XDHyp:\HostingUnits\MyHostingUnits\newNetwork.network'

        HostingUnitUid      : bcd3d649-86d1-4aa8-8ec2-d322b6a2c457
        HostingUnitName     : MyHostingUnit
        HypervisorConnection : MyConnection
        RootPath            : /
        RootId              :
        NetworkPath         : /Network 0.network
        NetworkId           : ab47080b-ca15-771a-c8dc-6ad9650158f1
        Storage             : {/Local storage.storage}
        PersonalvDiskStorage : {}
        VMTaggingEnabled    : True
        Metadata            : {}
        PermittedNetworks   : {/Network 0.network, /newNetwork.network}
```

The command adds a new network called "newNetwork.network" to the current directory. The dot (.) represents the current location (not its contents).

---------- EXAMPLE 3 ----------

```
XDHyp:\HostingUnits\MyHostingUnit>dir *.network | Add-HypHostingUnitNetwork -LiteralPath XDHyp:\HostingUnits\MyHostingUnit
```

The command adds all of the networks that are available in the hosting unit to the specified hosting unit.

---------- **EXAMPLE 4** ----------

```
c:\PS>Add-HypHostingUnitNetwork -LiteralPath XDHyp:\HostingUnits\MyHostingUnit -NetworkPath 'XDHyp:\HostingUnits\MyHostingUnits\newNetwork.network'

        HostingUnitUid      : bcd3d649-86d1-4aa8-8ec2-d322b6a2c457
        HostingUnitName     : MyHostingUnit
        HypervisorConnection : MyConnection
        RootPath            : /
        RootId              :
        NetworkPath         : /Network 0.network
        NetworkId           : ab47080b-ca15-771a-c8dc-6ad9650158f1
        Storage             : {/Local storage.storage}
        PersonalvDiskStorage : {}
        VMTaggingEnabled    : True
        Metadata            : {}
        PermittedNetworks   : {/Network 0.network, /newNetwork.network}
```

The command adds a new network location called "newNetwork.network" to the hosting unit called "MyHostingUnit".

Add-HypHostingUnitStorage

Sep 10, 2014

Adds storage locations to a hosting unit.

Syntax

Add-HypHostingUnitStorage [-LiteralPath] <String> [-StoragePath] <String> [-StorageType <StorageType>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Use this command to add storage locations for storing the hard disks required by the virtual machines created by the Citrix Machine Creation Service. You cannot use this command if the connection for the hosting unit is in maintenance mode.

Related topics

New-Item

Add-HypMetadata

remove-HypHostingUnitStorage

Parameters

-LiteralPath<String>

Specifies the path to the hosting unit to which storage will be added. The path must be in one of the following formats: <drive>:\HostingUnits\<HostingUnitName> or <drive>:\HostingUnits\{<HostingUnit Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	false

-StoragePath<String>

Specifies the path to the storage that will be added. The path must be in one of the following formats: <drive>:\Connections\<ConnectionName>\MyStorage.storage or <drive>:\Connections\{<Connection Uid>}\MyStorage.storage or <drive>:\HostingUnits\<HostingUnitName>\MyStorage.storage or <drive>:\HostingUnits\{<hostingUnit Uid>}\MyStorage.storage

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-StorageType<StorageType>

Specifies the type of storage in StoragePath. Supported storage types are: OSStorage PersonalvDiskStorage

Required?	false
Default Value	OSStorage
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. This can be a host name or an IP address.

Required?	false

Default Value	LocalHost. When a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Add-HypHostingUnitStorage (StoragePath parameter).

Return Values

Citrix.Host.Sdk.HostingUnit

Add-HypHostingUnitStorage returns an object containing the new definition of the hosting unit.

HostingUnitUid <Guid>

Specifies the unique identifier for the hosting unit.

HostingUnitName <string>

Specifies the name of the hosting unit.

HypervisorConnection <Citrix.Host.Sdk.HypervisorConnection>

Specifies the connection that the hosting unit uses to access a hypervisor.

RootId <string>

Identifies, to the hypervisor, the root of the hosting unit.

RootPath <string>

The hosting unit provider path that represents the root of the hosting unit.

Storage <Citrix.Host.Sdk.Storage[]>

The list of storage items that the hosting unit can use.

PersonalvDiskStorage <Citrix.XDPowerShell.Storage[]>

The list of storage items that the hosting unit can use for storing personal data.

VMTaggingEnabled <Boolean>

Specifies whether or not the metadata in the hypervisor can be used to store information about the XenDesktop Machine Creation Service.

NetworkId <string>

The hypervisor's internal identifier that represents the network specified for the hosting unit.

NetworkPath <string>

The hosting unit provider path to the network specified for the hosting unit.

Metadata <Citrix.Host.Sdk.Metadata[]>

A list of key value pairs that can store additional information about the hosting unit.

Notes

The storage path must be valid for the hosting unit. The rules that are applied are as follows: XenServer (HypervisorConnection Type = XenServer)

NA

VMWare vSphere/ESX (HypervisorConnection Type = vCenter)

The storage path must be directly contained in the root path item of the hosting unit.

Microsoft SCVMM/Hyper-v (HypervisorConnection Type = SCVMM)

Only one storage entry for these connection types is valid, and it must reference an SMB share. Additionally, if a Hyper-V failover cluster is used the SMB share must be the top-level mount point of the cluster shared volume on one of the servers in the cluster (i.e. C:\ClusterStorage).

In the case of failure, the following errors can result.

Error Codes

HostingUnitsPathInvalid

The path provided is not to an item in a subdirectory of a hosting unit item.

HostingUnitStoragePathInvalid

The specified path is invalid.

HostingUnitStoragePathInvalid

The storage path cannot be found or is invalid. See notes above about validity.

HostingUnitStorageDuplicateObjectExists

The specified storage path is already part of the hosting unit.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation. Communication with the database failed for

various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-HypHostingUnitStorage -LiteralPath XDHyp:\HostingUnits\MyHostingUnit -StoragePath 'XDHyp:\HostingUnits\MyHostingUnits\newStorage.storage'

        HostingUnitUid      : bcd3d649-86d1-4aa8-8ec2-d322b6a2c457
        HostingUnitName     : MyHostingUnit
        HypervisorConnection : MyConnection
        RootPath            : /
        RootId              :
        NetworkPath         : /Network 0.network
        NetworkId           : ab47080b-ca15-771a-c8dc-6ad9650158f1
        Storage             : {/Local storage.storage, /newStorage.storage}
        PersonalvDiskStorage : {/newStorage.storage}
        VMTaggingEnabled    : True
        Metadata            : {}
```

The command adds a new storage location called "newStorage.storage" to the hosting unit called "MyHostingUnit".

---------- EXAMPLE 2 ----------

```
XDHyp:\HostingUnits\MyHostingUnit>Add-HypHostingUnitStorage -LiteralPath . -StoragePath 'XDHyp:\HostingUnits\MyHostingUnits\newStorage.storage' -StorageType OSS

        HostingUnitUid      : bcd3d649-86d1-4aa8-8ec2-d322b6a2c457
        HostingUnitName     : MyHostingUnit
        HypervisorConnection : MyConnection
        RootPath            : /
        RootId              :
        NetworkPath         : /Network 0.network
        NetworkId           : ab47080b-ca15-771a-c8dc-6ad9650158f1
        Storage             : {/Local storage.storage, /newStorage.storage}
        PersonalvDiskStorage : {/Local storage.storage}
        VMTaggingEnabled    : True
        Metadata            : {}
```

The command adds a new storage location called "newStorage.storage" to the current directory. The dot (.) represents the current location (not its contents).

---------- EXAMPLE 3 ----------

```
XDHyp:\HostingUnits\MyHostingUnit>dir *.storage | Add-HypHostingUnitStorage -LiteralPath XDHyp:\HostingUnits\MyHostingUnit
```

The command adds all of the storage that is available in the hosting unit to the specified hosting unit.

---------- EXAMPLE 4 ----------

```
c:\PS>Add-HypHostingUnitStorage -LiteralPath XDHyp:\HostingUnits\MyHostingUnit -StoragePath 'XDHyp:\HostingUnits\MyHostingUnits\newStorage.storage' -StorageType

        HostingUnitUid      : bcd3d649-86d1-4aa8-8ec2-d322b6a2c457
        HostingUnitName     : MyHostingUnit
```

```
HypervisorConnection : MyConnection
RootPath             : /
RootId               :
NetworkPath          : /Network 0.network
NetworkId            : ab47080b-ca15-771a-c8dc-6ad9650158f1
Storage              : {/Local storage.storage}
PersonalvDiskStorage : {/Local storage.storage, /newStorage.storage}
VMTaggingEnabled     : True
Metadata             : {}
```

The command adds a new storage location called "newStorage.storage" to the hosting unit called "MyHostingUnit".

Add-HypHypervisorConnectionAddress

Sep 10, 2014

Add a connection address to a hypervisor connection.

Syntax

```
Add-HypHypervisorConnectionAddress [-LiteralPath] <String> [-HypervisorAddress] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to add addresses by which a hypervisor can be contacted. All addresses added to a single hypervisor connection are assumed to be equivalent (i.e. they all result in the ability to communicate with the same hypervisors). The hypervisor that the addresses reference is stored at the point of creation of the hypervisor connection. Once this is done, to be valid, all addresses must resolve to this hypervisor.

The addresses required are; XenServer - The address of the XenServer machines (must all reference the same XenServer pool). VMWare vSphere/ESX - The address of a vCenter Server. Microsoft SCVMM/Hyper-V - the address of an SCVMM server.

Related topics

Remove-HypHypervisorConnectionAddress

Get-HypXenServerAddress

Parameters

-LiteralPath<String>

Specifies the path within a Host Service provider to the hypervisor connection item to which to add the address. The path specified must be in one of the following formats; <drive>:\Connections\<HypervisorConnectionName> or <drive>:\Connections\{HypervisorConnection Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	false

-HypervisorAddress<String>

Specifies the address to be used. The address will be validated and the hypervisor must be contactable at the address supplied.

XenServer (ConnectionType = XenServer) The address being added must reference the same XenServer pool referenced by any existing addresses for the same connection. VMware vSphere\ESX (ConnectionType = vCenter) The address being added must be to the same VMware vCenter as the existing addresses. SCVMM\Hyper-v (ConnectionType = SCVMM) The address being added must be to the same SCVMM server as the existing addresses. Custom Connection Types ?Validation here I assume none need to check? #PUBS NOTE: ASSUME THIS TO BE UPDATED?#

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Host.Sdk.HypervisorConnection

Add-HypHypervisorConnectionAddress returns an object containing the new definition of the hypervisor connection.

HypervisorConnectionUid <Guid>

Specifies the unique identifier for the hypervisor connection.

HypervisorConnectionName <string>

Specifies the name of the hypervisor connection.

ConnectionType <Citrix.XDInterServiceTypes.ConnectionType>

Specifies the connection type of the connection.

XenServer - A Citrix XenServer hypervisor

SCVMM - A Microsoft SCVMM/Hyper-V hypervisor

vCenter - A VMWare vSphere/ESX hypervisor

Custom - A 3rd party hypervisor

HypervisorAddress <string[]>

A list of addresses that can be used to communicate with the hypervisor.

UserName <string>

The user name that is used when connecting to the hypervisor.

Persistent <Boolean>

Indicates whether the connection is stored in the database or is a temporary connection only with the same lifetime as the current Powershell session.

PlugInId <string>

The Citrix identifier for the Citrix Machine Management plug-in.

Revision <Guid>

Identifier for the current version of the hypervisor connection. This value changes every time a property of the hypervisor connection is updated.

SupportsPvsVMs <Boolean>

Indicates whether or not the connection can be used as part of a hosting unit and therefore used by the Citrix XenDesktop Machine Creation Service to

create virtual machines. Only the built-in supported hypervisor connection types can be used for this (i.e. XenServer, SCVMM and vCenter).

Metadata <Citrix.Host.Sdk.Metadata[]>

A list of key value pairs that can store additional information relating to the hosting unit.

Notes

The address format must be valid for the hypervisor connection. The rules that are applied are as below: XenServer (HypervisorConnection Type = XenServer)

http:\\<IP Address>

or http:\\<server Name>

or https:\\<server Name>

Note: To use multiple addresses to the same XenServer pool to provide failover functionality, all XenServers in the pool must have a shared block storage device. If the use of https connections and failover is required, the certificates on the servers must be trusted by all of the controllers (typically this means having a root certificate installed).

VMWare vSphere/ESX (HypervisorConnection Type = vCenter)

http:\\<IP Address>\<sdk path>

http:\\<server Name>\<sdk path>

or https:\\<Server Name>\<sdk path>

Notes:

* Http requires manual vCenter configuration; https is the only supported default format.

* Default sdk path is 'sdk'

Microsoft SCVMM/Hyper-v (HypervisorConnection Type = SCVMM)

IP Address

server Name (short or FQDN)

Note: If XenServers are moved to new XenServer pools after being added to a hypervisor connection, unpredictable results can occur. Once a XenServer is assigned to a hypervisor connection, it must not be moved to a new XenServer pool.

In the case of failure the following errors can result.

Error Codes

InputConnectionsPathInvalid

The path provided is not to an item in a sub directory of a hosting unit item.

HypervisorConnectionAddressForeignKeyObjectDoesNotExist

The hypervisor connection to which the address is to be added could not be located.

ConnectionAddressInvalid

The address could not be used to contact a hypervisor or the validation rules have not been met.

HypervisorConnectionAddressDuplicateObjectExists

The address specified is already part of the hypervisor connection.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for

various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-HypHypervisorConnectionAddress -LiteralPath XDHyp:\Connections\MyConnection -HypervisorAddress http:\\myserver.com

PSPath               : Citrix.HostingUnitService.Admin.V1.0\Citrix.Hypervisor::XDHyp:\Connections\MyConnection
PSParentPath         : Citrix.HostingUnitService.Admin.V1.0\Citrix.Hypervisor::XDHyp:\Connections
PSChildName          : MyConnection
PSDrive              : XDHyp
PSProvider           : Citrix.HostingUnitService.Admin.V1.0\Citrix.Hypervisor
PSIsContainer        : True
HypervisorConnectionUid : 85581f42-c5da-4976-970c-ebc3448ea1e3
HypervisorConnectionName : MyConnection
ConnectionType       : XenServer
HypervisorAddress    : {http:\\myserver2.com,http:\\myserver.com}
UserName             : root
Persistent           : False
PluginId             : XenFactory
SupportsPvsVMs       : True
Revision             : 4c95c857-c54d-4f92-abef-0cce32c02502
Metadata             :
```

Add the address 'http:\\myserver.com' to the hypervisor connection called "MyConnection".

Add-HypHypervisorConnectionMetadata

Sep 10, 2014

Adds metadata on the given HypervisorConnection.

Syntax

Add-HypHypervisorConnectionMetadata [-HypervisorConnectionUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHypervisorConnectionMetadata [-HypervisorConnectionUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHypervisorConnectionMetadata [-HypervisorConnectionName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHypervisorConnectionMetadata [-HypervisorConnectionName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHypervisorConnectionMetadata [-InputObject] <HypervisorConnection[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHypervisorConnectionMetadata [-InputObject] <HypervisorConnection[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given HypervisorConnection objects. This cmdlet will not overwrite existing metadata on an object - use the Set-HypHypervisorConnectionMetadata cmdlet instead.

Related topics

Set-HypHypervisorConnectionMetadata

Remove-HypHypervisorConnectionMetadata

Parameters

-HypervisorConnectionUid<Guid>

Id of the HypervisorConnection

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HypervisorConnectionName<String>

Name of the HypervisorConnection

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<HypervisorConnection[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the HypervisorConnection specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Host.Sdk.Metadata

Add-HypHypervisorConnectionMetadata returns an array of objects containing the new definition of the metadata.

\n Property <string>

\n Specifies the name of the property.

\n Value <string>

\n Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DuplicateObject

One of the specified metadata already exists.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Add-HypHypervisorConnectionMetadata -HypervisorConnectionUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Property                       Value
        --------                      -----
        property                       value
```

Add metadata with a name of 'property' and a value of 'value' to the HypervisorConnection with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Add-HypHypervisorConnectionScope

Sep 10, 2014

Add the specified HypervisorConnection(s) to the given scope(s).

Syntax

```
Add-HypHypervisorConnectionScope [-Scope] <String[]> -InputObject <HypervisorConnection[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHypervisorConnectionScope [-Scope] <String[]> -HypervisorConnectionUid <Guid[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-HypHypervisorConnectionScope [-Scope] <String[]> -HypervisorConnectionName <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The AddHypHypervisorConnectionScope cmdlet is used to associate one or more HypervisorConnection objects with given scope(s).

There are multiple parameter sets for this cmdlet, allowing you to identify the HypervisorConnection objects in different ways:

- HypervisorConnection objects can be piped in or specified by the InputObject parameter

- The HypervisorConnectionUid parameter specifies objects by HypervisorConnectionUid

- The HypervisorConnectionName parameter specifies objects by HypervisorConnectionName (supports wildcards)

To add a HypervisorConnection to a scope you need permission to change the scopes of the HypervisorConnection and permission to add objects to all of the scopes you have specified.

If the HypervisorConnection is already in a scope, that scope will be silently ignored.

Related topics

Remove-HypHypervisorConnectionScope

Get-HypScopedObject

Parameters

-Scope<String[]>

Specifies the scopes to add the objects to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-InputObject<HypervisorConnection[]>

Specifies the HypervisorConnection objects to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HypervisorConnectionUid<Guid[]>

Specifies the HypervisorConnection objects to be added by HypervisorConnectionUid.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HypervisorConnectionName<String[]>

Specifies the HypervisorConnection objects to be added by HypervisorConnectionName.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

None

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

ScopeNotFound

One of the specified scopes was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command with the specified objects or scopes.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-HypHypervisorConnectionScope Finance -HypervisorConnectionUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
```
Adds a single HypervisorConnection to the 'Finance' scope.

---------- EXAMPLE 2 ----------

```
c:\PS>Add-HypHypervisorConnectionScope Finance,Marketing -HypervisorConnectionUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
```
Adds a single HypervisorConnection to the multiple scopes.

---------- EXAMPLE 3 ----------

```
c:\PS>Get-HypHypervisorConnection | Add-HypHypervisorConnectionScope Finance
```
Adds all visible HypervisorConnection objects to the 'Finance' scope.

---------- EXAMPLE 4 ----------

```
c:\PS>Add-HypHypervisorConnectionScope Finance -HypervisorConnectionName A*
```
Adds HypervisorConnection objects with a name starting with an 'A' to the 'Finance' scope.

Add-HypMetadata

Sep 10, 2014

Adds metadata to a hypervisor connection or a hosting unit.

Syntax

Add-HypMetadata [-LiteralPath] <String> [-Property] <String> [-Value] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Use this command to store additional custom data against a hosting unit or hypervisor connection. This data is not used by the Machine Creation Service, and is provided only for consumers of the services to store any data that may be required for their operations. The metadata is returned along with the hypervisor connection or hosting unit that it is assigned to.

Related topics

Remove-HypMetadata

Parameters

-LiteralPath<String>

Specifies the path within a hosting unit provider to the hosting unit or hypervisor connection item to which to add the metadata. The path specified must be in one of the following formats: <drive>:\HostingUnits\<HostingUnitName> or <drive>:\HostingUnits\{<HostingUnit Uid> or <drive>:\Connections\<Connection Name> or <drive>:\Connections\{<Connection Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Property<String>

Specifies the property name of the metadata to be added. The property must be unique for the item specified by the path.

The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string the contains a path to Add-HypMetadata (Path parameter).

Return Values

Citrix.Host.Sdk.Metadata

Add-HypMetadata returns an object containing the new definition of the metadata.

Property <string>

Specifies the property of the metadata.

Value <string>

Specifies the value of the metadata.

Notes

In the case of failure, the following errors can result.

Error Codes

InvalidPath

The path provided is not in the required format.

HostingUnitMetadataForeignKeyObjectDoesNotExist

The hosting unit supplied in the path does not exist.

HypervisorConnectionMetadataForeignKeyObjectDoesNotExist

The hypervisor connection supplied in the path does not exist.

HostingUnitMetadataDuplicateObjectExists

Metadata for the specified hosting unit item already exists with the same property name.

HypervisorConnectionMetadataDuplicateObjectExists

Metadata for the specified hypervisor connection item already exists with the same property name.

MetadataContainerUndefined

The specified path does not reference a hosting unit or a hypervisor connection.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the

XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-HypMetadata -LiteralPath XDHyp:\Connections\MyConnection -Property MyProperty -Value MyValue

Property                                 Value
--------                                 -----
MyProperty                                MyValue
```

The command adds the metadata with the property name of "MyProperty" and value of "MyValue" to the hypervisor connection item called "MyConnection".

---------- EXAMPLE 2 ----------

```
c:\PS>dir xdhyp\connections\Citrix* | Add-HypMetadata -Property MyProperty -Value MyValue

Property                                 Value
--------                                 -----
MyProperty                                MyValue
MyProperty                                MyValue
MyProperty                                MyValue
```

The command adds the metadata with the property name of "MyProperty" and value of "MyValue" to all the hypervisor connection items that begin with the string "Citrix".

Get-HypConfigurationDataForItem

Sep 10, 2014

Retrieves the configuration data for an item in the Host Service provider path. Note: For this release, only VM items are supported for this operation.

Syntax

```
Get-HypConfigurationDataForItem [-LiteralPath] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This command provides a mechanism for retrieving extra data about an entry in the hosting unit service provider. The referenced item must be contained within the connections directory in the provider (i.e. XDHyp:\Connections).

This mechanism is used for obtaining data that is not required frequently and/or has a high overhead associated with its retrieval (so as to maintain the responsiveness of the provider). For this release of the PowerShell snap-in, the only provider items that can be used with this operation are VM items. For a VM, this provides a mechanism to obtain the number of CPUs, the amount of Memory (in MB) and hard disk drive capacity (in GB).

Related topics

Get-Item

Parameters

-LiteralPath<String>

Specifies the path within a hosting unit provider to the item for which configuration data is to be retrieved. The path specified must be in one of the following formats; <drive>:\Connections\<Connection Name>\<Item Path of VM object> or <drive>:\Connections\{<connection Uid>\<Item Path of VM object>} or <drive>:\HostingUnits\<HostingUnit Name>\<Item Path of VM object> or <drive>:\HostingUnits\{<hostingUnit Uid>\<Item Path of VM object>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Get-HypConfigurationDataForItem

Return Values

PSObject

Get-HypConfigurationDataForItem returns a PSObject containing the properties that are appropriate for the item specified by the path.

Properties for VM Item

CPUCount <int>

Specifies the number of CPUs assigned to the VM.

MemoryMB <int>

The amount of memory allocated to the VM.

HardDiskSizeGB <int>

The capacity of the primary hard drive assigned to the VM.

Notes

For this release, this cmdlet provides only configuration data for VM objects in the provider. Using a path to an item that is not a VM results in a error.

In the case of failure the following errors can result.

Error Codes

InputHypervisorItemPathInvalid

The path provided is not to an item in a sub-directory of a connection item or a hosting unit item.

InvalidHypervisorItemPath

No item exists with the specified path.

InvalidHypervisorItem

The item specified by the path exists, but is not a VM Item.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

CommunicationError

An error occurred while communicating with the service.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

HypervisorPermissionDenied

The hypervisor login used does not provide authorization to access the data for this item.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\MyConnection\MyVm.vm

                CpuCount                MemoryMB                HardDiskSizeGB
                --------                --------                --------------
                    1                    1024                    24
```

This command gets the configuration properties for a VM called 'MyVm.vm' within a hypervisor connection called 'MyConnection'.

---------- EXAMPLE 2 ----------

```
XDHyp:\HostingUnits\PS>Get-HypConfigurationDataForItem -LiteralPath .\MyVm.vm

                CpuCount                MemoryMB                HardDiskSizeGB
                --------                --------                --------------
                    1                    1024                    24
```

This command gets the configuration properties for a VM called 'MyVm.vm' within the current directory. The dot (.) represents the current location (not its contents).

---------- EXAMPLE 3 ----------

```
C:\PS>(Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\MyConnection\MyVm.vm).CPUCount
```

This command gets the CPU count for a VM called 'MyVm.vm'. The CPUCount is just one property of the VM items. To see all properties of an item, type "(Get-HypConfigurationDataForItem <ItemPath>) | Get-Member".

Get-HypConfigurationObjectForItem

Sep 10, 2014

Retrieves the configuration data for an item in the Host Service provider path. Note: For this release, only VM items are supported for this operation.

Syntax

```
Get-HypConfigurationObjectForItem [-LiteralPath] <String> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

This command provides a mechanism for retrieving extra data about an entry in the hosting unit service provider. The referenced item must be contained within the connections directory in the provider (i.e. XDHyp:\Connections).

This mechanism is used for obtaining data that is not required frequently and/or has a high overhead associated with its retrieval (so as to maintain the responsiveness of the provider). For this release of the PowerShell snap-in the only provider items that can be used with this operation are VM items. For a VM this provides a mechanism to obtain the number of CPUs, the amount of Memory (in MB) and hard disk drive capacity (GB).

Related topics

Get-Item

Parameters

-LiteralPath<String>

Specifies the path within a hosting unit provider to the item for which configuration data is to be retrieved. The path specified must be in one of the following formats; <drive>:\Connections\<Connection Name>\<Item Path of VM object> or <drive>:\Connections\{<connection Uid>\<Item Path of VM object>} or <drive>:\HostingUnits\<HostingUnit Name>\<Item Path of VM object> or <drive>:\HostingUnits\{<hostingUnit Uid>\<Item Path of VM object>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value will become the default.

Accept Pipeline Input?	false

Input Type

System.string You can pipe a string the contains a path to Get-HypConfigurationDataForItem

Return Values

PSObject

Get-HypConfigurationDataForItem returns a PSObject containing the properties that are appropriate for the item specified by the path.

Properties for VM Item

CPUCount <int>

Specifies the number of CPUs assigned to the VM.

MemoryMB <int>

The amount of memory allocated to the VM.

HardDiskSizeGB <int>

The capacity of the primary hard drive assigned to the VM.

Network Map

The networks that this Vm or Snaphot is connected to

Notes

For this release this cmdlet only provides configuration data for VM objects in the provider. Using a path to an item that is not a VM will result in a error.

In the case of failure the following errors can be produced.

Error Codes

InputHypervisorItemPathInvalid

The path provided is not to an item in a sub directory of a connection item or a hosting unit item.

InvalidHypervisorItemPath

No item exists with the specified path.

InvalidHypervisorItem

The item specified by the path exists, but is not a VM Item.

DatabaseError

An error occurred in the service whilst attempting a database operation.

DatabaseNotConfigured

The operation could not be completed as the database for the service is not configured.

DataStoreException

An error occurred in the service whilst attempting a database operation - communication to database failed for

for various reasons.

CommunicationError

An error occurred whilst communicating with the service.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

HypervisorPermissionDenied

The hypervisor login used does not provide authorization to access the data for this item.

ExceptionThrown

An unexpected error occurred. To locate more details see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\MyConnection\MyVm.vm

                CpuCount                MemoryMB                HardDiskSizeGB
                --------                --------                --------------
                    1                    1024                    24
```

This command gets the configuration properties for a VM called 'MyVm.vm' within a hypervisor connection called 'MyConnection'.

---------- EXAMPLE 2 ----------

```
XDHyp:\HostingUnits\PS>Get-HypConfigurationDataForItem -LiteralPath .\MyVm.vm

                CpuCount                MemoryMB                HardDiskSizeGB
                --------                --------                --------------
                    1                    1024                    24
```

This command gets the configuration properties for a VM called 'MyVm.vm' within the current directory. The dot (.) represents the current location (not its contents).

---------- EXAMPLE 3 ----------

```
C:\PS>(Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\MyConnection\MyVm.vm).CPUCount
```

This command gets the CPU count for a VM called 'MyVm.vm'. The CPUCount is just one property of the VM items. To see all properties of an item, type "(Get-HypConfigurationDataForItem <ItemPath>) | Get-Member".

Get-HypConnectionRegion

Sep 10, 2014

Enumerates the regions of a hypervisor connection that are based on cloud technology.

Syntax

```
Get-HypConnectionRegion [-LiteralPath] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to enumerate the available regions within a public or private cloud, when making hypervisor connections to cloud services. Sometimes, regions need to be selected and applied before the cloud connection can be used in a meaningful way. This cmdlet allows the supported regions to be listed so that one may be selected.

Once a region has been chosen, use the standard Set-Item provider cmdlet to select it. See the examples for further details.

This cmdlet may return no output, in which case the cloud connection can be considered "regionless" (or, implicitly, all within a single region). In such cases, there is no need to select a region, and the hypervisor connection can be used as is.

Related topics

Set-Item

Parameters

-LiteralPath<String>

Specifies the path to the hypervisor connection whose regions are being examined. This cmdlet is valid only for hypervisor connections that have the UsesCloudInfrastructure flag set to true. The path must be in one of the following formats: <drive>:\Connections\<ConnectionName> or <drive>:\Connections\{<Connection Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide a host name or an IP address.

Required?	false
Default Value	LocalHost. When a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Get-HypConnectionRegion (LiteralPath parameter).

Return Values

Citrix.Host.Sdk.HypervisorRegion

Get-HypConnectionRegion returns zero or more instances of the HypervisorConnectionRegion object, each of which contain the following properties:

Name <string> Specifies the unique name of the region. Endpoint <string> Specifies the URL endpoint that is specific to the region, if relevant. This may be an empty string, and is returned only for information purposes.

A full list of the hypervisor networks that are exposed for use in the hosting unit.

Notes

In the case of failure, the following errors can be produced.

Error Codes

ConnectionsPathInvalid

The path provided is not to an item in the Connections subdirectory of the host service provider.

HypervisorConnectionObjectNotFound

The path provided could not be resolved to an existing hypervisor connection. The name or GUID is invalid.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

ConnectionIsNotCloud

The hypervisor connection is not associated with cloud infrastructure, making it invalid to enumerate regions.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation. Communication with the database failed for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-HypConnectionRegions -LiteralPath XDHyp:\Connections\AWS

        RegionName        : us-east-1
        Endpoint          : ec2.us-east-1.amazonaws.com

        RegionName        : us-west-1
        Endpoint          : ec2.us-west-1.amazonaws.com

        RegionName        : eu-west-1
        Endpoint          : ec2.eu-west-1.amazonaws.com

        (...)

        c:\PS>Set-Item -Path XDHyp:\Connections\AWS -Region "us-east-1"
```

This sequence of commands enumerates the available regions of an Amazon AWS cloud connection, and then selects one of them for use in the connection.

Get-HypDBConnection

Sep 10, 2014

Gets the database string for the specified data store used by the Host Service.

Syntax

```
Get-HypDBConnection [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the database connection string for the specified data store.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

Related topics

Get-HypServiceStatus

Set-HypDBConnection

Test-HypDBConnection

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

system.string

The database connection string configured for the Host Service.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the Host Service has not been specified.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-HypDBConnection

Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True
```

Get the database connection string for the Host Service.

Get-HypDBSchema

Sep 10, 2014

Gets a script that creates the Host Service database schema for the specified data store.

Syntax

Get-HypDBSchema [-DatabaseName <String>] [-ServiceGroupName <String>] [-ScriptType <ScriptTypes>] [-LocalDatabase] [-Sid <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets SQL scripts that can be used to create a new Host Service database schema, add a new Host Service to an existing site, remove a Host Service from a site, or create a database server logon for a Host Service. If no Sid parameter is provided, the scripts obtained relate to the currently selected Host Service instance, otherwise the scripts relate to Host Service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied. The current service instance is that on the local machine, or that explicitly specified by the last usage of the -AdminAddress parameter to a Host SDK cmdlet. The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured. The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SMDCMD mode'. The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to Host Service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to Host Service roles

If ScriptType is Evict, the returned script contains:

o Removal of Host Service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database. You do not need to configure a database before using this command.

Related topics

Set-HypDBConnection

Parameters

-DatabaseName<String>

Specifies the name of the database for which the schema will be generated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the Host services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<ScriptTypes>

Specifies the type of database script returned. Available script types are:

Database

Returns a full database script that can be used to create a database schema for the Host Service in a database instance that does not already contain a schema for this service. The DatabaseName and ServiceGroupName parameters must be specified to create a script of this type.

Instance

Returns a permissions script that can be used to add further Host services to an existing database instance that already contains the full Host service schema, associating the services to the Service Group. The Sid parameter can optionally be specified to create a script of this type.

Login

Returns a database logon script that can be used to add the required logon accounts to an existing database instance that contains the Host Service schema. This is used primarily when creating a mirrored database environment. The

DatabaseName parameter must be specified to create a script of this type.

Evict

Returns a script that can be used to remove the specified Host Service from the database entirely. The DatabaseName and Sid parameters must be specified to create a script of this type.

Required?	false
Default Value	Database
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for Host services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Sid<String>

Specifies the SID of the controller on which the Host Service instance to remove from the database is running.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.string

A string containing the required SQL script for application to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-HypDBSchema -DatabaseName MyDB -ServiceGroupName  MyServiceGroup > c:\HypSchema.sql
```

Get the full database schema for site data store of the Host Service and copy it to a file called 'c:\HypSchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a Host Service site schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-HypDBSchema -DatabaseName MyDB -scriptType Login > c:\HostLogins.sql
```

Get the logon scripts for the Host Service.

Get-HypDBVersionChangeScript

Sep 10, 2014

Gets a script that updates the Host Service database schema.

Syntax

```
Get-HypDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a database script that can be used to upgrade or downgrade the site or secondary schema for the Host Service from the current schema version to a different version.

Related topics

Get-HypInstalledDBVersion

Parameters

-DatabaseName<String>

Specifies the name of the database instance to which the update applies.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

Specifies the version of the database you want to update to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

A PSObject containing the required SQL script for application to a database.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any Host services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-HypServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Host Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS> $update = Get-HypDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-HypHypervisorPlugin

Sep 10, 2014

Gets the available hypervisor types.

Syntax

```
Get-HypHypervisorPlugin [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to retrieve a list of all the available hypervisor types, and their localized names.

Related topics

New-Item

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Host.Sdk.HypervisorPlugin

Get-HypHypervisorPlugin returns a list of objects containing the definition of the hypervisor plug-ins.

ConnectionType <Citrix.XDInterServiceTypes.ConnectionType>

The hypervisor connection type. This can be one of the following:

XenServer - XenServer hypervisor

SCVMM - Microsoft SCVMM/Hyper-V

vCenter - VMWare vSphere/ESX

Custom - a third-party hypervisor

DisplayName <string>

The localized display name (localized using the locale of the Powershell snap-in session)

PluginFactoryName <string>

The name of the hypervisor plug-in factory used to manage the hypervisor connections.

Notes

To use third-party plug-ins, the plug-in assemblies must be installed into the appropriate location on each controller machine that forms part of the Citrix controller site. Failure to do this can result in unpredictable behavior, especially during service failover conditions.

In the case of failure the following errors can result.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

CommunicationError

An error occurred while communicating with the service.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS> Get-HypHypervisorPlugin | Format-Table -AutoSize

        ConnectionType DisplayName           PluginFactoryName
        -------------- -----------           -----------------
                 SCVMM Microsoft virtualization MicrosoftPSFactory
               VCenter VMware virtualization    VmwareFactory
             XenServer Citrix XenServer         XenFactory
```

Get the available hypervisor management plug-ins.

Get-HypInstalledDBVersion

Sep 10, 2014

Gets a list of all available database schema versions for the Host Service.

Syntax

```
Get-HypInstalledDBVersion [-Upgrade] [-Downgrade] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the current version of the Host Service database schema, if no flags are set, otherwise returns versions for which upgrade or downgrade scripts are available and have been stored in the database.

Related topics

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Version

The Get-HypInstalledDbVersion command returns objects containing the new definition of the Host Service database schema version.

Major <Integer>

Minor <Integer>

Build <Integer>

Revision <Integer>

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Host Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-HypInstalledDBVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      6      0      0
```

Get the currently installed version of the Host Service database schema.

-------------------------- EXAMPLE 2 --------------------------

```
c:\PS>Get-HypInstalledDBVersion -Upgrade

Major  Minor  Build  Revision
-----  -----  -----  --------
6      0      0      0
```

Get the versions of the Host Service database schema for which upgrade scripts are supplied.

Get-HypScopedObject

Sep 10, 2014

Gets the details of the scoped objects for the Host Service.

Syntax

Get-HypScopedObject [-ScopeId <Guid>] [-ScopeName <String>] [-ObjectType <ScopedObjectType>] [-ObjectId <String>] [-ObjectName <String>] [-Description <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns a list of directly scoped objects including the names and identifiers of both the scope and object as well as the object description for display purposes.

There will be at least one result for every directly scoped object. When an object is associated with multiple scopes the output contains one result per scope duplicating the object details.

No records are returned for the All scope, though if an object is not in any scope a result with a null ScopeId and ScopeName will be returned.

Related topics

Parameters

-ScopeId<Guid>

Gets scoped object entries for the given scope identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ScopeName<String>

Gets scoped object entries with the given scope name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ObjectType<ScopedObjectType>

Gets scoped object entries for objects of the given type.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ObjectId<String>

Gets scoped object entries for objects with the specified object identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ObjectName<String>

Gets scoped object entries for objects with the specified object identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Gets scoped object entries for objects with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Hyp_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Hyp_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Host.Sdk.ScopedObject

The Get-HypScopedObject command returns an object containing the following properties:

ScopeId <Guid?>

Specifies the unique identifier of the scope.

ScopeName <String>

Specifies the display name of the scope.

ObjectType <ScopedObjectType>

Type of the object this entry relates to.

ObjectId <String>

Unique identifier of the object.

ObjectName <String>

Display name of the object

Description <String>

Description of the object (possibly $null if the object type does not have a description).

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-HypScopedObject -ObjectType Scheme

ScopeId    : eff6f464-f1ee-4442-add3-99982e0cec01
ScopeName  : Sales
ObjectType : Scheme
ObjectId   : cd4174ee-9e4b-4e57-b126-9dbf757fe493
ObjectName : MyExampleScheme
Description : Test scheme

ScopeId    : 304e0fa7-d390-47f0-a94f-7e956a324c41
ScopeName  : Finance
ObjectType : Scheme
ObjectId   : cd4174ee-9e4b-4e57-b126-9dbf757fe493
ObjectName : MyExampleScheme
Description : Test scheme

ScopeId    :
ScopeName  :
ObjectType : Scheme
ObjectId   : 5062e46b-71bc-4ac9-901a-30fe6797e2f6
ObjectName : AnotherScheme
Description : Another scheme in no scopes
```

Gets all of the scoped objects with type Scheme. The example output shows a scheme object (MyExampleScheme) in two scopes Sales and Finance, and another scheme (AnotherScheme) that is not in any scope. The ScopeId and ScopeName values returned are null in the final record.

Get-HypService

Sep 10, 2014

Gets the service record entries for the Host Service.

Syntax

Get-HypService [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns instances of the Host Service that the service publishes. The service records contain account security identifier information that can be used to remove each service from the database.

A database connection for the service is required to use this command.

Related topics

Parameters

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Hyp_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Hyp_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Host.Sdk.Service

The Get-HypServiceInstance command returns an object containing the following properties.

Uid <Integer>

Specifies the unique identifier for the service in the group. The unique identifier is an index number.

ServiceHostId <Guid>

Specifies the unique identifier for the service instance.

DNSName <String>

Specifies the domain name of the host on which the service runs.

MachineName <String>

Specifies the short name of the host on which the service runs.

CurrentState <Citrix.Fma.Sdk.ServiceCore.ServiceState>

Specifies whether the service is running, started but inactive, stopped, or failed.

LastStartTime <DateTime>

Specifies the date and time at which the service was last restarted.

LastActivityTime <DateTime>

Specifies the date and time at which the service was last stopped or restarted.

OSType

Specifies the operating system installed on the host on which the service runs.

OSVersion

Specifies the version of the operating system installed on the host on which the service runs.

ServiceVersion

Specifies the version number of the service instance. The version number is a string that reflects the full build version of the service.

DatabaseUserName <string>

Specifies for the service instance the Active Directory account name with permissions to access the database. This will be either the machine account or, if the database is running on a controller, the NetworkService account.

Sid <string>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

ActiveSiteServices <string[]>

Specifies the names of active site services currently running in the service. Site services are components that perform long-running background processing in some services. This field is empty for services that do not contain site services.

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-HypService

Uid             : 1
ServiceHostId     : aef6f464-f1ee-4042-a523-66982e0cecd0
DNSName           : MyServer.company.com
MachineName       : MYSERVER
CurrentState      : On
LastStartTime     : 04/04/2011 15:25:38
LastActivityTime  : 04/04/2011 15:33:39
OSType            : Win32NT
OSVersion         : 6.1.7600.0
ServiceVersion    : 5.1.0.0
DatabaseUserName  : NT AUTHORITY\NETWORK SERVICE
SID               : S-1-5-21-2316621082-1546847349-2782505528-1165
ActiveSiteServices : {MySiteService1, MySiteService2...}
```

Get all the instances of the Host Service running in the current service group.

Get-HypServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the Host Service on the controller.

Syntax

```
Get-HypServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the Host Service on the controller to be detected.

You do not need to configure a database connection before using this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

List containing added capabilities.

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-HypServiceAddedCapability
```

Get the added capabilities of the Host Service.

Get-HypServiceInstance

Sep 10, 2014

Gets the service instance entries for the Host Service.

Syntax

Get-HypServiceInstance [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns service interfaces published by the instance of the Host Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Host.Sdk.ServiceInstance

The Get-HypServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

\n Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

\n Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

\n Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a

central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

\n Specifies the service instance type. For this service, the service instance type is always Hyp.

Address

\n Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

\n Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

\n Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

\n Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

\n Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

\n Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

\n SDK - for PowerShell operations

\n InterService - for operations between different services

\n Peer - for communications between services of the same type

Metadata <Citrix.Host.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-HypServiceInstance

Address          : http://MyServer.com:80/Citrix/SdkHostingUnitService
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         :
MetadataMap      :
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName  : MyServiceGroup
ServiceGroupUid   : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType      : Hyp
Version          : 1

Address          : http://MyServer.com:80/Citrix/SdkHostingUnitService/IServiceApi
Binding          : wcf_HTTP_kerb
InterfaceType    : InterService
Metadata         :
MetadataMap      :
```



```
ServiceAccount     : ENG\MyAccount
ServiceAccountSid  : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName   : MyServiceGroup
ServiceGroupUid    : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType        : Hyp
Version            : 1
```

Get all instances of the Host Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-HypServiceStatus

Sep 10, 2014

Gets the current status of the Host Service on the controller.

Syntax

```
Get-HypServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the Host Service on the controller to be monitored. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured.

Related topics

Set-HypDBConnection

Test-HypDBConnection

Get-HypDBConnection

Get-HypDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-HypServiceStatus command returns an object containing the status of the Host Service together with extra diagnostics information.

DBUnconfigured

The Host Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the Host Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Host Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Host Service currently in use is incompatible with the version of the Host Service schema on the database. Upgrade the Host Service to a more recent version.

DBOlderVersionThanService

The version of the Host Service schema on the database is incompatible with the version of the Host Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Host Service is running and is connected to a database containing a valid schema.

Failed

The Host Service has failed.

Unknown

(0) The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-HypServiceStatus
```

DBUnconfigured
Get the current status of the Host Service.

Get-HypVMMacAddress

Sep 10, 2014

Retrieves a list the MAC addresses for the VMs in the specified connection.

Syntax

```
Get-HypVMMacAddress [-LiteralPath] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to obtain a list of MAC addresses of all the virtual machines in the specified connection.

Related topics

Get-Item

Parameters

-LiteralPath<String>

The path to a connection item in the hosting provider. Paths to anything other than a connection item will result in an error being returned. The path can be provided as either <drive>:\connections\<Connection Name> or <drive:>\connections\{<Connection Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Get-HypConfigurationDataForItem

Return Values

Citrix.Host.Sdk.HypervisorVMObject

Get-HypVMMMacAddress returns an object containing the following properties.

MacAddress <string> - specifies the MAC address of the VM.

VMId <string> - specifies the identifier for the VM as defined in the hypervisor hosting it.

Notes

The path must refer to a connection item. Hosting unit items are not valid.

In the case of failure, the following errors can result.

Error Codes

InputConnectionsPathInvalid

If the path is not provided in an expected format, an InputConnectionsPathInvalid error results.

HypervisorConnectionObjectNotFound

The hypervisor connection object specified cannot be found.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

CommunicationError

An error occurred while communicating with the service.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS>Get-HypVMMacAddress -LiteralPath XDHyp:\Connections\MyConnection

MacAddress                VMId
----------                ----
52:b0:1c:ed:60:fa          f3395d2a-a196-41c2-e37d-764acf871599
62:6f:f0:40:d5:af          5f4457b0-cc3c-f806-8ca7-5f57e4bdf2d1
4e:a5:9f:00:b2:0c          3115177b-85a9-d8ee-d0f9-0c7437483c09
```

This command gets the MAC addresses for the connection called "MyConnection".

-------------------------- EXAMPLE 2 --------------------------

```
XDHyp:\Connections\MyConnection>Get-HypVMMacAddress -Path .

MacAddress                VMId
----------                ----
52:b0:1c:ed:60:fa          f3395d2a-a196-41c2-e37d-764acf871599
62:6f:f0:40:d5:af          5f4457b0-cc3c-f806-8ca7-5f57e4bdf2d1
4e:a5:9f:00:b2:0c          3115177b-85a9-d8ee-d0f9-0c7437483c09
```

This command gets the MAC addresses for the connection at the current directory. The dot (.) represents the current location (not its contents).

-------------------------- EXAMPLE 3 --------------------------

```
C:\PS>Get-HypVMMacAddress -LiteralPath Xdhyp:\connections\"{268c66db-9b8c-47f6-9265-42326dbff006}"
```

This command gets the MAC addresses for the connection that has a ConnectionUid of 268c66db-9b8c-47f6-9265-42326dbff006.

Get-HypVolumeServiceConfiguration

Sep 10, 2014

Gets instances of the VolumeServiceConfiguration that are configured for this site.

Syntax

Get-HypVolumeServiceConfiguration [[-VolumeServiceConfigurationName] <String>] [-VolumeServiceConfigurationUid <Guid>] [-ConnectionType <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Retrieve VolumeServiceConfigurations whose properties match the given filter criteria. If no parameters are specified, this cmdlet retrieves all VolumeServiceConfiguration objects.

Related topics

Set-HypVolumeServiceConfiguration

Parameters

-VolumeServiceConfigurationName<String>

Specifies a filter for the configuration name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-VolumeServiceConfigurationUid<Guid>

Specifies a filter for the configuration ID.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ConnectionType<String>

Specifies a filter for the cloud connection type, such as "AWS" or "CloudPlatform".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Hyp_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false

Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Hyp_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

string The name of a configuration (or set of configurations) to retrieve.

Return Values

Citrix.Host.Sdk.VolumeServiceConfiguration

This cmdlet returns matching VolumeServiceConfiguration objects.

Examples

---------- EXAMPLE 1 ----------

C:\PS>Get-HypVolumeServiceConfiguration -VolumeServiceConfigurationName SiteDefault -ConnectionType CloudPlatform
This command lists the site default volume service configuration for connections that use Citrix Cloud Platform.

Get-HypXenServerAddress

Sep 10, 2014

Gets all the available addresses for a XenServer hypervisor connection.

Syntax

Get-HypXenServerAddress [-LiteralPath] <String> [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Use this cmdlet to retrieve all the available hypervisor connection addresses that can be used to connect to the same XenServer pool. When used in conjunction with Add-HypHypervisorAddress, you can easily populate a connection with all the addresses that can be used to provide full failover support for a XenServer connection.

If the addresses are https addresses, the command uses the certificates installed on the XenServers to provide suitable https addresses where possible. Only servers that can be resolved are returned.

Related topics

Add-HypHypervisorConnectionAddress

Parameters

-LiteralPath<String>

Specifies the path within a Host Service provider to the hypervisor connection item to which to add the address. The path specified must be in one of the following formats: <drive>:\Connections\<HypervisorConnectionName> or <drive>:\Connections\{HHypervisorConnection Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.string

Get-HypXenServerAddress returns a list of strings containing the available address.

Notes

For this to work as required with https connections, the certificates installed on the XenServers must be trusted by all controllers. Typically this means having the root certificate for the certificate trust chain installed on all controllers. Wildcard certificates are not supported for this operation.

In the case of failure, the following errors can result.

Error Codes

InputConnectionsPathInvalid

The path provided is not to an item in a sub-directory of a hosting unit item.

HypervisorConnectionNotXenServer

The hypervisor connection to which the path refers is not for a Citrix XenServer hypervisor.

HypervisorConnectionObjectNotFound

The hypervisor connection at the path specified cannot be located.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for

various reasons.

CommunicationError

An error occurred while communicating with the service.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-HypXenServerAddress -Path XDHyp:\Connections\MyConnection

https:\\myserver.com
https:\\myServer1.com
```

Gets the available addresses for the connection "MyConnection".

---------- EXAMPLE 2 ----------

```
c:\PS>Get-HypXenServerAddress -LiteralPath XDHyp:\Connections\MyConnection | Add-HypHypervisorConnectionAddress -Path XDHyp:\Connections\MyConnectionPath
```

Adds all the available addresses for the XenServer pool in "MyConnection" to the hypervisor connection.

Grant-HypSecurityGroupEgress

Sep 10, 2014

Adds an egress rule to a security group.

Syntax

Grant-HypSecurityGroupEgress [-LiteralPath] <String> -GroupId <String[]> -Protocol <String> [-FromPort <Decimal>] [-ToPort <Decimal>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Grant-HypSecurityGroupEgress [-LiteralPath] <String> -IPRange <String[]> -Protocol <String> [-FromPort <Decimal>] [-ToPort <Decimal>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Adding an egress rule permits network traffic from instances within the security group to pass to one or more destination CIDR IP address ranges or security groups.

Related topics

Amazon AuthorizeSecurityGroupEgress: http://docs.aws.amazon.com/AWSEC2/latest/APIReference/ApiReference-query-AuthorizeSecurityGroupEgress.html

IANA protocol numbers: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Grant-HypSecurityGroupIngress

Revoke-HypSecurityGroupIngress

Revoke-HypSecurityGroupEgress

Parameters

-LiteralPath<String>

Specifies the full XDHyp provider path to the security group, equivalent to the FullPath property of the security group object. The path can specify a security group relative to a hypervisor conection or hosting unit.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Protocol<String>

Specifies the protocol name or number. Protocol numbers can be found at: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Use -1 to specify all protocols.

Required?	true
Default Value	
Accept Pipeline Input?	false

-GroupId<String[]>

Specifies one or more destination security groups to which traffic will be permitted by this rule. This parameter cannot be specified in conjunction with IPRange.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IPRange<String[]>

Specifies one or more destination CIDR IP address ranges to which traffic will be permitted by this rule. This parameter cannot be specified in conjunction with IPRange.

Required?	true
Default Value	
Accept Pipeline Input?	false

-FromPort<Decimal>

The start of the port range for port based protocols. For ICMP this specifies the type number.

Use -1 to specify all ICMP types.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-ToPort<Decimal>

The end of the port range for port based protocols. For ICMP this specifies the type number, where -1 can be used to specify all ICMP types.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string The LiteralPath can be piped in.

Return Values

None

Notes

Security groups can be added and removed using the New-Item and Remove-Item cmdlets.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS> $Group = New-Item -ItemType SecurityGroup -Path XDHyp:\Connections\AWS -Name MySecurityGroup -Description 'Example group'
       c:\PS> Grant-HypSecurityGroupEgress $Group.FullPath -Protocol '-1' -IPRange '0.0.0.0/16'
```

Create a security group and grant full egress to anywhere.

---------- EXAMPLE 2 ----------

```
c:\PS> $Group1 = New-Item -ItemType SecurityGroup -Path XDHyp:\Connections\AWS -Name MySecurityGroup1 -Description 'Example group 1'
       c:\PS> $Group2 = New-Item -ItemType SecurityGroup -Path XDHyp:\Connections\AWS\MySecurityGroup2 -Description 'Example group 2'
       c:\PS> Grant-HypSecurityGroupEgress $Group1.FullPath -FromPort 0 -ToPort 0 -Protocol icmp -GroupId $Group2.Id
       c:\PS> Grant-HypSecurityGroupIngress $Group2.FullPath -FromPort 0 -ToPort 0 -Protocol icmp -GroupId $Group1.Id
```

Make 2 security groups and permit group 1 to ping group 2.

Grant-HypSecurityGroupIngress

Sep 10, 2014

Adds an ingress rule to a security group.

Syntax

Grant-HypSecurityGroupIngress [-LiteralPath] <String> -GroupId <String[]> -Protocol <String> [-FromPort <Decimal>] [-ToPort <Decimal>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Grant-HypSecurityGroupIngress [-LiteralPath] <String> -IPRange <String[]> -Protocol <String> [-FromPort <Decimal>] [-ToPort <Decimal>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Adding an egress rule permits network traffic from source CIDR IP address ranges or security groups to pass to instances within a security group.

Related topics

Amazon AuthorizeSecurityGroupEgress: http://docs.aws.amazon.com/AWSEC2/latest/APIReference/ApiReference-query-AuthorizeSecurityGroupEgress.html

IANA protocol numbers: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Grant-HypSecurityGroupEgress

Revoke-HypSecurityGroupIngress

Revoke-HypSecurityGroupEgress

Parameters

-LiteralPath<String>

Specifies the full XDHyp provider path to the security group, equivalent to the FullPath property of the security group object. The path can specify a security group relative to a hypervisor conection or hosting unit.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Protocol<String>

Specifies the protocol name or number. Protocol numbers can be found at: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Use -1 to specify all protocols.

Required?	true
Default Value	
Accept Pipeline Input?	false

-GroupId<String[]>

Specifies one or more source security groups from which traffic will be permitted by this rule. This parameter cannot be specified in conjunction with IPRange.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IPRange<String[]>

Specifies one or more source CIDR IP address ranges from which traffic will be permitted by this rule. This parameter cannot be specified in conjunction with IPRange.

Required?	true
Default Value	
Accept Pipeline Input?	false

-FromPort<Decimal>

The start of the port range for port based protocols. For ICMP this specifies the type number.

Use -1 to specify all ICMP types.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-ToPort<Decimal>

The end of the port range for port based protocols. For ICMP this specifies the type number, where -1 can be used to specify all ICMP types.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string The LiteralPath can be piped in.

Return Values

None

Notes

Security groups can be added and removed using the New-Item and Remove-Item cmdlets.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS> $Group = New-Item -ItemType SecurityGroup -Path XDHyp:\Connections\AWS -Name MySecurityGroup -Description 'Example group'
       c:\PS> Grant-HypSecurityGroupIngress $Group.FullPath -FromPort 80 -ToPort 80 -Protocol tcp -IPRange '0.0.0.0/0'
```

Create a security group and grant ingress on port 80 from anywhere.

---------- EXAMPLE 2 ----------

```
c:\PS> $Group1 = New-Item -ItemType SecurityGroup -Path XDHyp:\Connections\AWS -Name MySecurityGroup1 -Description 'Example group 1'
       c:\PS> $Group2 = New-Item -ItemType SecurityGroup -Path XDHyp:\Connections\AWS\MySecurityGroup2 -Description 'Example group 2'
       c:\PS> Grant-HypSecurityGroupEgress $Group1.FullPath -FromPort 8080 -ToPort 8080 -Protocol tcp -GroupId $Group2.Id
       c:\PS> Grant-HypSecurityGroupIngress $Group2.FullPath -FromPort 8080 -ToPort 8080 -Protocol tcp -GroupId $Group1.Id
       c:\PS> Grant-HypSecurityGroupEgress $Group2.FullPath -Protocol '-1' -GroupId $Group1.Id
       c:\PS> Grant-HypSecurityGroupIngress $Group1.FullPath -Protocol '-1' -GroupId $Group2.Id
```

Make 2 security groups and permit group 1 access to group 2 only on port 8080 while granting full access to group 1 from group 2.

New-HypVMSnapshot

Sep 10, 2014

Creates a new snapshot for the specified VM item path.

Syntax

```
New-HypVMSnapshot [-LiteralPath] <String> [-SnapshotName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [[-SnapshotDescription] <String>] [<CommonParameters>]
```

Detailed Description

Use this command to create a new snapshot of a virtual machine, for a given Host Service provider path to a VM. The resulting snapshot can then be used for operations that require a snapshot to work.

Related topics

Parameters

-LiteralPath<String>

Specifies the path within a hosting unit provider to the virtual machine item for which to create a new snapshot. The path specified must be in one of the following formats: <drive>:\Connections\<Connection Name>\<Item Path of VM object> or <drive>:\Connections\{<connection Uid>\<Item Path of VM object>} or <drive>:\HostingUnits\<HostingUnit Name>\<Item Path of VM object> or <drive>:\HostingUnits\{<hostingUnit Uid>\<Item Path of VM object>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-SnapshotName<String>

The name of the new snapshot. This is visible in the hypervisor management console.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

-SnapshotDescription<String>

The description to add to the snapshot. This is visible in the hypervisor management console.

Required?	false

Default Value	
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Get-HypConfigurationDataForItem

Return Values

System.string.

The provider path to the newly created snapshot.

Notes

In the case of failure, the following errors can result.

Error Codes

InputHypervisorItemPathInvalid

The path provided is not to an item in a sub-directory of a connection item or a hosting unit item.

InvalidHypervisorItemPath

No item exists with the specified path.

InvalidHypervisorItem

The item specified by the path exists, but is not a VM Item.

SnapshotNameAlreadyInUse

The specified name is already in use and will cause a name resolution clash.

FailedToCreateSnapshot

The snapshot creation process failed.

HypervisorInMaintenanceMode

The hypervisor is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for

various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

SnapshotChainTooLong

Snapshot creation failed. Snapshot chain is too long.

SnapshotCreationNotAuthorized

Snapshot creation failed. User not authorized to create snapshots.

Examples

---------- EXAMPLE 1 ----------


```
C:\PS>New-HypVMSnapshot -LiteralPath XDHyp:\Connections\MyConnection\MyVm.vm -SnapshotName "New snapshot" -SnapshotDescription "Example snapshot"

                XDHyp:\Connections\MyConnection\MyVm.vm\New snapshot.snapshot
```

This command creates a snapshot of a VM called 'MyVm.vm' within a hypervisor connection called 'MyConnection'.

Remove-HypHostingUnitMetadata

Sep 10, 2014

Removes metadata from the given HostingUnit.

Syntax

Remove-HypHostingUnitMetadata [-HostingUnitUid] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHostingUnitMetadata [-HostingUnitUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHostingUnitMetadata [-HostingUnitName] <String> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHostingUnitMetadata [-HostingUnitName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHostingUnitMetadata [-InputObject] <HostingUnit[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHostingUnitMetadata [-InputObject] <HostingUnit[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to remove metadata from the given HostingUnit.

Related topics

Add-HypHostingUnitMetadata

Set-HypHostingUnitMetadata

Parameters

-HostingUnitUid<Guid>

Id of the HostingUnit

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HostingUnitName<String>

Name of the HostingUnit

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<HostingUnit[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create

high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-HypHostingUnit | % { Remove-HypHostingUnitMetadata -Map $_.MetadataMap }
```

Remove all metadata from all HostingUnit objects.

Remove-HypHostingUnitNetwork

Sep 10, 2014

Removes networks from a hosting unit.

Syntax

```
Remove-HypHostingUnitNetwork [-LiteralPath] <String> [-NetworkPath] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to remove networks from a hosting unit. This does not remove the network from the hypervisor, only the reference to the network for the Host Service. After it is removed, the network is no longer available for associating with virtual NICs (when creating new virtual machines with the Machine Creation Service). Any virtual machines that have been created already continue to use the network until they are removed from the deployment. This command cannot be used if the connection for the hosting unit is in maintenance mode. If the network to be removed no longer exists on the hypervisor for the hosting unit, you must supply a fully qualified path to the network location.

Related topics

Add-HypHostingUnitNetwork

Parameters

-LiteralPath<String>

Required?	true
Default Value	
Accept Pipeline Input?	false

-NetworkPath<String>

Specifies the path in the hosting unit provider of the network to remove. The path specified must be in one of the following formats: <drive>:\Connections\<HostingUnitName>\MyNetwork.network or <drive>:\Connections\{<hostingUnit Uid>}\MyNetwork.network

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. This can be a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Remove-HypHostingUnitNetwork (Path parameter).

Notes

In the case of failure, the following errors can result.

Error Codes

HostingUnitsPathInvalid

The path provided is not to an item in a subdirectory of a hosting unit item.

HostingUnitNetworkObjectToDeleteDoesNotExist

The network path specified is not part of the hosting unit.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation. Communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Remove-HypHostingUnitNetwork -LiteralPath XDHyp:\HostingUnits\MyHostingUnit -NetworkPath 'XDHyp:\HostingUnits\MyHostingUnits\newNetwork.network'
```

The command removes the network called "newNetwork.network" from the hosting unit called "MyHostingUnit"

Remove-HypHostingUnitStorage

Sep 10, 2014

Removes storage from a hosting unit.

Syntax

Remove-HypHostingUnitStorage [-LiteralPath] <String> [-StoragePath <String>] [-StorageType <StorageType>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Use this command to remove storage locations from a hosting unit. This does not remove the storage from the hypervisor, only the reference to the storage for the Host Service. After removal, the storage is no longer used to store hard disks (when creating new virtual machines with the Machine Creation Service). The hard disks located already on the storage remain in place and virtual machines that have been created already continue to use the storage until they are removed from the deployment. Do not use this command if the connection for the hosting unit is in maintenance mode. If the storage location to be removed no longer exists on the hypervisor for the hosting unit, you must supply a fully qualified path to the storage location.

Related topics

Add-HypHostingUnitStorage

Parameters

-LiteralPath<String>

Required?	true
Default Value	
Accept Pipeline Input?	false

-StoragePath<String>

Specifies the path in the hosting unit provider of the storage to remove. If StoragePath is not specified, all storage is removed from the hosting unit. The path specified must be in one of the following formats: <drive>:\Connections\<HostingUnitName>\MyStorage.storage or <drive>:\Connections\{<hostingUnit Uid>}\MyStorage.storage

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-StorageType<StorageType>

Specifies the type of storage in StoragePath. Supported storage types are: OSStorage PersonalvDiskStorage

Required?	false
Default Value	OSStorage
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. This can be a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Remove-HypHostingUnitStorage (Path parameter).

Notes

After storage is removed, it is the administrator's responsibility to maintain its contents. The Citrix XenDesktop Machine Creation Service does not attempt to clean up any data that is stored in the storage location.

If all storage is removed from the hosting unit, other features of the Machine Creation Service stops functioning until some storage is added again.

In the case of failure, the following errors can result.

Error Codes

HostingUnitsPathInvalid

The path provided is not to an item in a subdirectory of a hosting unit item.

HostingUnitStorageObjectToDeleteDoesNotExist

The storage path specified is not part of the hosting unit.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation. Communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Remove-HypHostingUnitStorage -LiteralPath XDHyp:\HostingUnits\MyHostingUnit -StoragePath 'XDHyp:\HostingUnits\MyHostingUnits\newStorage.storage'
```

The command removes the OS storage location called "newStorage.storage" from the hosting unit called "MyHostingUnit"

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ChildItem XDHYP:\HostingUnits\Host\*.storage | Remove-HypHostingUnitStorage XDHYP:\HostingUnits\Host1
```

The command removes all OS storage from all hosting units called "Host1".

---------- EXAMPLE 3 ----------

```
c:\PS>Get-ChildItem XDHYP:\HostingUnits\Host\*.storage | Remove-HypHostingUnitStorage -StorageType PersonalvDiskStorage
```

The command removes all PersonalvDisk storage from all hosting units called "Host1".

Remove-HypHypervisorConnectionAddress

Sep 10, 2014

Removes addresses from the list of available connection addresses.

Syntax

```
Remove-HypHypervisorConnectionAddress [-LiteralPath] <String> [-HypervisorAddress] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to remove addresses that can be used to connect to the hypervisor specified by the hypervisor connection. If all addresses are removed, the connection cannot be used until a valid address is added to the hypervisor connection.

Related topics

Add-HypHypervisorConnectionAddress

Parameters

-LiteralPath<String>

Specifies the path within a Host Service provider to the hosting unit item to which to add the address. The path specified must be in one of the following formats: <drive>:\HostingUnits\<HostingUnitName> or <drive>:\HostingUnits\{HostingUnit Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	false

-HypervisorAddress<String>

Specifies the address to be removed. If this parameter is not provided, all addresses are removed from the hypervisor connection.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Remove-HypHypervisorConnectionAddress (Path parameter).

Notes

Changes to a hypervisor connection affect all entities that reference the connection. If all addresses are removed from the connection, any other entities that reference the hypervisor connection (e.g. hosting units) cannot make new connections to the hypervisor.

In the case of failure, the following errors can result.

Error Codes

InputConnectionsPathInvalid

The path provided is not to an item in a subdirectory of a hosting unit item.

HypervisorConnectionAddressForeignKeyObjectDoesNotExist

The hypervisor connection to which the address is to be added could not be located.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for

various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Remove-HypHypervisorConnectionAddress -LiteralPath XDHyp:\HostingUnits\MyHypervisorConnection -HypervisorAddress 'http:\\myserver.com'
```

The command removes the address "http:\\myserver.com" from the hypervisor connection called "MyHypervisorConnection".

---------- EXAMPLE 2 ----------

```
c:\PS>Get-Item –Path XDHYP:\Connections\* | Remove-HypHypervisorConnectionAddress
```

The command removes all addresses from all the hypervisor connections currently defined.

Remove-HypHypervisorConnectionMetadata

Sep 10, 2014

Removes metadata from the given HypervisorConnection.

Syntax

Remove-HypHypervisorConnectionMetadata [-HypervisorConnectionUid] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHypervisorConnectionMetadata [-HypervisorConnectionUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHypervisorConnectionMetadata [-HypervisorConnectionName] <String> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHypervisorConnectionMetadata [-HypervisorConnectionName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHypervisorConnectionMetadata [-InputObject] <HypervisorConnection[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHypervisorConnectionMetadata [-InputObject] <HypervisorConnection[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to remove metadata from the given HypervisorConnection.

Related topics

Add-HypHypervisorConnectionMetadata

Set-HypHypervisorConnectionMetadata

Parameters

-HypervisorConnectionUid<Guid>

Id of the HypervisorConnection

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HypervisorConnectionName<String>

Name of the HypervisorConnection

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<HypervisorConnection[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-HypHypervisorConnection | % { Remove-HypHypervisorConnectionMetadata -Map $_.MetadataMap }
```

Remove all metadata from all HypervisorConnection objects.

Remove-HypHypervisorConnectionScope

Sep 10, 2014

Remove the specified HypervisorConnection(s) from the given scope(s).

Syntax

```
Remove-HypHypervisorConnectionScope [-Scope] <String[]> -InputObject <HypervisorConnection[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHypervisorConnectionScope [-Scope] <String[]> -HypervisorConnectionUid <Guid[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypHypervisorConnectionScope [-Scope] <String[]> -HypervisorConnectionName <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The RemoveHypHypervisorConnectionScope cmdlet is used to remove one or more HypervisorConnection objects from the given scope(s).

There are multiple parameter sets for this cmdlet, allowing you to identify the HypervisorConnection objects in different ways:

- HypervisorConnection objects can be piped in or specified by the InputObject parameter

- The HypervisorConnectionUid parameter specifies objects by HypervisorConnectionUid

- The HypervisorConnectionName parameter specifies objects by HypervisorConnectionName (supports wildcards)

To remove a HypervisorConnection from a scope you need permission to change the scopes of the HypervisorConnection.

If the HypervisorConnection is not in a specified scope, that scope will be silently ignored.

Related topics

Add-HypHypervisorConnectionScope

Get-HypScopedObject

Parameters

-Scope<String[]>

Specifies the scopes to remove the objects from.

Required?	true
Default Value	
Accept Pipeline Input?	false

-InputObject<HypervisorConnection[]>

Specifies the HypervisorConnection objects to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HypervisorConnectionUid<Guid[]>

Specifies the HypervisorConnection objects to be removed by HypervisorConnectionUid.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HypervisorConnectionName<String[]>

Specifies the HypervisorConnection objects to be removed by HypervisorConnectionName.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

None

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

ScopeNotFound

One of the specified scopes was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command with the specified objects or scopes.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Remove-HypHypervisorConnectionScope Finance -HypervisorConnectionUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
```

Removes a single HypervisorConnection from the 'Finance' scope.

---------- EXAMPLE 2 ----------

```
c:\PS>Remove-HypHypervisorConnectionScope Finance,Marketing -HypervisorConnectionUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
```

Removes a single HypervisorConnection from multiple scopes.

---------- EXAMPLE 3 ----------

```
c:\PS>Get-HypHypervisorConnection | Remove-HypHypervisorConnectionScope Finance
```

Removes all visible HypervisorConnection objects from the 'Finance' scope.

---------- EXAMPLE 4 ----------

```
c:\PS>Remove-HypHypervisorConnectionScope Finance -HypervisorConnectionName A*
```

Removes HypervisorConnection objects with a name starting with an 'A' from the 'Finance' scope.

Remove-HypMetadata

Sep 10, 2014

Removes metadata from a hypervisor connection or hosting unit.

Syntax

```
Remove-HypMetadata [-LiteralPath] <String> [-Property <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to remove custom data from a specific hosting unit or hypervisor connection. If the Property parameter is not provided, all metadata is removed from the specified item.

Related topics

Remove-HypMetadata

Parameters

-LiteralPath<String>

Specifies the path within a Host Service provider to the hosting unit or hypervisor connection item from which to remove the metadata. The path specified must be in one of the following formats: <drive>:\HostingUnits\<HostingUnitName> or <drive>:\HostingUnits\{<HostingUnit Uid> or <drive>:\Connections\<Connection Name> or <drive>:\Connections\{<Connection Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Property<String>

Specifies the property name of the metadata to be removed.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Add-HypMetadata (Path parameter).

Notes

In the case of failure, the following errors can result.

Error Codes

InvalidPath

The path provided is not in the required format.

HostingUnitMetadataObjectToDeleteDoesNotExist

The hosting unit supplied in the path does not exist.

HypervisorConnectionObjectToDeleteDoesNotExist

The hypervisor connection supplied in the path does not exist.

MetadataContainerUndefined

The specified path does not reference a hosting unit or a hypervisor connection.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Remove-HypMetadata -LiteralPath XDHyp:\Connections\MyConnection -Property MyProperty
```

The command removes the metadata with the property "MyProperty" from the hypervisor connection called "MyConnection".

---------- EXAMPLE 2 ----------

```
C:\PS>Remove-HypMetadata -LiteralPath XDHyp:\Connections\MyConnection
```

The command removes all the metadata from the hypervisor connection called "MyConnection".

---------- EXAMPLE 3 ----------

```
C:\PS>dir XDHyp:\connections | Remove-HypMetadata
```

The command removes all the metadata from all the hypervisor connections.

Remove-HypServiceMetadata

Sep 10, 2014

Removes metadata from the given Service.

Syntax

```
Remove-HypServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypServiceMetadata [-ServiceHostId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypServiceMetadata [-InputObject] <Service[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-HypServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Service.

Related topics

Set-HypServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-HypService | % { Remove-HypServiceMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Service objects.

Reset-HypServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the Host Service.

Syntax

```
Reset-HypServiceGroupMembership [-ConfigServiceInstance] <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Enables you to reload Host Service access permissions and configuration service locations. The Reset-HypServiceGroupMembership command must be run on at least one instance of the service type (Hyp) after installation and registration with the configuration service. Without this operation, the Host services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-HypServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Parameters

-ConfigServiceInstance<ServiceInstance[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.Host.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-HypServiceGroupMembership command.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-HypServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-HypServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Revoke-HypSecurityGroupEgress

Sep 10, 2014

Removes an egress rule from a security group.

Syntax

Revoke-HypSecurityGroupEgress [-LiteralPath] <String> -GroupId <String[]> -Protocol <String> [-FromPort <Decimal>] [-ToPort <Decimal>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Revoke-HypSecurityGroupEgress [-LiteralPath] <String> -IPRange <String[]> -Protocol <String> [-FromPort <Decimal>] [-ToPort <Decimal>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

To remove a rule, specify parameters matching an existing rule's values.

Related topics

Amazon AuthorizeSecurityGroupEgress: http://docs.aws.amazon.com/AWSEC2/latest/APIReference/ApiReference-query-AuthorizeSecurityGroupEgress.html

IANA protocol numbers: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Grant-HypSecurityGroupIngress

Grant-HypSecurityGroupEgress

Revoke-HypSecurityGroupIngress

Parameters

-LiteralPath<String>

Specifies the full XDHyp provider path to the security group, equivalent to the FullPath property of the security group object. The path can specify a security group relative to a hypervisor conection or hosting unit.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Protocol<String>

Specifies the protocol name or number. Protocol numbers can be found at: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Use -1 to specify all protocols.

Required?	true
Default Value	
Accept Pipeline Input?	false

-GroupId<String[]>

Specifies one or more destination security groups to which traffic will be permitted by this rule. This parameter cannot be specified in conjunction with IPRange.

Required?	true
Default Value	

Accept Pipeline Input?	false

-IPRange<String[]>

Specifies one or more destination CIDR IP address ranges to which traffic will be permitted by this rule. This parameter cannot be specified in conjunction with IPRange.

Required?	true
Default Value	
Accept Pipeline Input?	false

-FromPort<Decimal>

The start of the port range for port based protocols. For ICMP this specifies the type number.

Use -1 to specify all ICMP types.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-ToPort<Decimal>

The end of the port range for port based protocols. For ICMP this specifies the type number, where -1 can be used to specify all ICMP types.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Input Type

System.string The LiteralPath can be piped in.

Return Values

None

Notes

Security groups cannot be removed in AWS if they are referened by rules from other security groups.

Security groups can be added and removed using the New-Item and Remove-Item cmdlets.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS> $Group = New-Item -ItemType SecurityGroup -Path XDHyp:\Connections\AWS -Name MySecurityGroup -Description 'Example group'
       c:\PS> Grant-HypSecurityGroupEgress $Group.FullPath -Protocol '-1' -IPRange '0.0.0.0/0'
       c:\PS> Revoke-HypSecurityGroupEgress $Group.FullPath -Protocol '-1' -IPRange '0.0.0.0/0'
       c:\PS> Remove-Item $Group.FullPath
```

Create a security group, grant full egress to anywhere, then revoke access and delete the security group.

Revoke-HypSecurityGroupIngress

Sep 10, 2014

Removes an ingress rule from a security group.

Syntax

Revoke-HypSecurityGroupIngress [-LiteralPath] <String> -GroupId <String[]> -Protocol <String> [-FromPort <Decimal>] [-ToPort <Decimal>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Revoke-HypSecurityGroupIngress [-LiteralPath] <String> -IPRange <String[]> -Protocol <String> [-FromPort <Decimal>] [-ToPort <Decimal>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

To remove a rule, specify parameters matching an existing rule's values.

Related topics

Amazon AuthorizeSecurityGroupEgress: http://docs.aws.amazon.com/AWSEC2/latest/APIReference/ApiReference-query-AuthorizeSecurityGroupEgress.html

IANA protocol numbers: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Grant-HypSecurityGroupIngress

Grant-HypSecurityGroupEgress

Revoke-HypSecurityGroupIngress

Parameters

-LiteralPath<String>

Specifies the full XDHyp provider path to the security group, equivalent to the FullPath property of the security group object. The path can specify a security group relative to a hypervisor conection or hosting unit.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Protocol<String>

Specifies the protocol name or number. Protocol numbers can be found at: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Use -1 to specify all protocols.

Required?	true
Default Value	
Accept Pipeline Input?	false

-GroupId<String[]>

Specifies one or more source security groups from which traffic will be permitted by this rule. This parameter cannot be specified in conjunction with IPRange.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IPRange<String[]>

Specifies one or more source CIDR IP address ranges from which traffic will be permitted by this rule. This parameter cannot be specified in conjunction with IPRange.

Required?	true
Default Value	
Accept Pipeline Input?	false

-FromPort<Decimal>

The start of the port range for port based protocols. For ICMP this specifies the type number.

Use -1 to specify all ICMP types.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-ToPort<Decimal>

The end of the port range for port based protocols. For ICMP this specifies the type number, where -1 can be used to specify all ICMP types.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string The LiteralPath can be piped in.

Return Values

None

Notes

Security groups cannot be removed in AWS if they are referened by rules from other security groups.

Security groups can be added and removed using the New-Item and Remove-Item cmdlets.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS> $Group1 = New-Item -ItemType SecurityGroup -Path XDHyp:\Connections\AWS -Name MySecurityGroup1 -Description 'Example group 1'
       c:\PS> $Group2 = New-Item -ItemType SecurityGroup -Path XDHyp:\Connections\AWS -Name MySecurityGroup2 -Description 'Example group 2'
       c:\PS> Grant-HypSecurityGroupEgress $Group1.FullPath -FromPort 8080 -ToPort 8085 -Protocol tcp -GroupId $Group2.Id
       c:\PS> Grant-HypSecurityGroupIngress $Group2.FullPath -FromPort 8080 -ToPort 8085 -Protocol tcp -GroupId $Group1.Id
       c:\PS> Revoke-HypSecurityGroupEgress $Group1.FullPath -FromPort 8080 -ToPort 8085 -Protocol tcp -GroupId $Group2.Id
       c:\PS> Revoke-HypSecurityGroupIngress $Group2.FullPath -FromPort 8080 -ToPort 8085 -Protocol tcp -GroupId $Group1.Id
```

Create 2 security groups, grant access from group 1 to group 2, then revoke access.

Set-HypAdminConnection

Sep 10, 2014

Set the controller to be used by the cmdlets that form the Host service PowerShell snap-in.

Syntax

```
Set-HypAdminConnection [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to set the default controller address to be used by the cmdlets to communicate with the controller. Most Host service cmdlets take an 'AdminAddress' parameter that can be used to define the controller (when used, this overrides this setting). However, the Set-Location cmdlet in the Host service provider does not offer this option. Therefore, the controller address must be set using this cmdlet, if no other cmdlets have set the address previously in the current runspace.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-HypAdminConnection -AdminAddress myserver.com
```

This command sets the controller address for the commands to be "myserver.com". All commands run use this address until it is altered, either by another call to this command or by the use of the 'AdminAddress' parameter in another command in the Host service snap-in.

Set-HypDBConnection

Sep 10, 2014

Configures a database connection for the Host Service.

Syntax

```
Set-HypDBConnection [-DBConnection] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Configures a connection to a database in which the Host Service can store its state. The service will attempt to connect and start using the database immediately after the connection is configured. The database connection string is updated to the specified value regardless of whether it is valid or not. Specifying an invalid connection string prevents a service from functioning until the error is corrected.

After a connection is configured, you cannot alter it without first clearing it (by setting the connection to $null).

You do not need to configure a database connection to use this command.

Related topics

Get-HypServiceStatus

Get-HypDBConnection

Test-HypDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the Host Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-HypDBConnection command returns an object containing the status of the Host Service together with extra diagnostics information.

DBUnconfigured

The Host Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the Host Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Host Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Host Service currently in use is incompatible with the version of the Host Service schema on the database. Upgrade the Host Service to a more recent version.

DBOlderVersionThanService

The version of the Host Service schema on the database is incompatible with the version of the Host Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Host Service is running and is connected to a database containing a valid schema.

Failed

The Host Service has failed.

Unknown

The status of the Host Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-HypDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Configures a database connection string for the Host Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Set-HypDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Configures an invalid database connection string for the Host Service.

Set-HypHostingUnitMetadata

Sep 10, 2014

Adds or updates metadata on the given HostingUnit.

Syntax

Set-HypHostingUnitMetadata [-HostingUnitUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHostingUnitMetadata [-HostingUnitUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHostingUnitMetadata [-HostingUnitName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHostingUnitMetadata [-HostingUnitName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHostingUnitMetadata [-InputObject] <HostingUnit[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHostingUnitMetadata [-InputObject] <HostingUnit[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given HostingUnit objects.

Related topics

Add-HypHostingUnitMetadata

Remove-HypHostingUnitMetadata

Parameters

-HostingUnitUid<Guid>

Id of the HostingUnit

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HostingUnitName<String>

Name of the HostingUnit

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<HostingUnit[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the HostingUnit specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-HypHostingUnitMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-HypHostingUnitMetadata -HostingUnitUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the HostingUnit with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-HypHostingUnitStorage

Sep 10, 2014

Sets options for a storage location on a hosting unit.

Syntax

Set-HypHostingUnitStorage [-LiteralPath] <String> [-StoragePath] <String> [-StorageType <StorageType>] [-Superseded <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Use this command to set options for storage locations that are defined for a hosting unit. Do not use this command if the connection for the hosting unit is in maintenance mode.

Related topics

Parameters

-LiteralPath<String>

Specifies the path to the hosting unit which defines the storage. The path must be in one of the following formats: <drive>:\HostingUnits\<HostingUnitName> or <drive>:\HostingUnits\{<HostingUnit Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	false

-StoragePath<String>

Specifies the path to the storage that will be modified. The path must be in one of the following formats: <drive>:\Connections\<ConnectionName>\MyStorage.storage or <drive>:\Connections\{<Connection Uid>}\MyStorage.storage or <drive>:\HostingUnits\<HostingUnitName>\MyStorage.storage or <drive>:\HostingUnits\{<hostingUnit Uid>}\MyStorage.storage

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-StorageType<StorageType>

Specifies the type of storage in StoragePath. Supported storage types are: OSStorage PersonalvDiskStorage

Required?	false
Default Value	OSStorage
Accept Pipeline Input?	false

-Superseded<Boolean>

Specifies that this storage has been superseded and must not be used for future provisioning operations. Existing virtual machines using this storage will continue to function.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects. This can be a host name or an IP address.

Required?	false
Default Value	LocalHost. When a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path to Add-HypHostingUnitStorage (StoragePath parameter).

Return Values

Citrix.XDPowerShell.HostingUnit

Add-HypHostingUnitStorage returns an object containing the new definition of the hosting unit.

HostingUnitUid <Guid>

Specifies the unique identifier for the hosting unit.

HostingUnitName <string>

Specifies the name of the hosting unit.

HypervisorConnection <Citrix.XDPowerShell.HypervisorConnection>

Specifies the connection that the hosting unit uses to access a hypervisor.

RootId <string>

Identifies, to the hypervisor, the root of the hosting unit.

RootPath <string>

The hosting unit provider path that represents the root of the hosting unit.

Storage <Citrix.XDPowerShell.Storage[]>

The list of storage items that the hosting unit can use.

PersonalvDiskStorage <Citrix.XDPowerShell.Storage[]>

The list of storage items that the hosting unit can use for storing personal data.

VMTaggingEnabled <Boolean>

Specifies whether or not the metadata in the hypervisor can be used to store information about the XenDesktop Machine Creation Service.

NetworkId <string>

The hypervisor's internal identifier that represents the network specified for the hosting unit.

NetworkPath <string>

The hosting unit provider path to the network specified for the hosting unit.

Metadata <Citrix.XDPowerShell.Metadata[]>

A list of key value pairs that can store additional information about the hosting unit.

Notes

The storage path must be valid for the hosting unit. The rules that are applied are as follows: XenServer (HypervisorConnection Type = XenServer)

NA

VMWare vSphere/ESX (HypervisorConnection Type = vCenter)

The storage path must be directly contained in the root path item of the hosting unit.

Microsoft SCVMM/Hyper-v (HypervisorConnection Type = SCVMM)

Only one storage entry for these connection types is valid, and it must reference an SMB share. Additionally, if a Hyper-V failover cluster is used the SMB share must be the top-level mount point of the cluster shared volume on one of the servers in the cluster (i.e. C:\ClusterStorage).

In the case of failure, the following errors can be produced.

Error Codes

HostingUnitsPathInvalid

The path provided is not to an item in a subdirectory of a hosting unit item.

HostingUnitStoragePathInvalid

The specified path is invalid.

HostingUnitStoragePathInvalid

The storage path cannot be found or is invalid. See notes above about validity.

HostingUnitStorageDuplicateObjectExists

The specified storage path is already part of the hosting unit.

HypervisorInMaintenanceMode

The hypervisor for the connection is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation. Communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-HypHostingUnitStorage -LiteralPath XDHyp:\HostingUnits\MyHostingUnit -StoragePath 'XDHyp:\HostingUnits\MyHostingUnits\newStorage.storage' -Superseded $

        HostingUnitUid      : bcd3d649-86d1-4aa8-8ec2-d322b6a2c457
        HostingUnitName     : MyHostingUnit
        HypervisorConnection : MyConnection
        RootPath            : /
        RootId              :
        NetworkPath         : /Network 0.network
        NetworkId           : ab47080b-ca15-771a-c8dc-6ad9650158f1
        Storage             : {/Local storage.storage, /newStorage.storage}
        PersonalvDiskStorage : {/newStorage.storage}
        VMTaggingEnabled    : True
        Metadata            : {}
```

The command updates a storage location called "newStorage.storage" associated with the hosting unit called "MyHostingUnit".

Set-HypHypervisorConnectionMetadata

Sep 10, 2014

Adds or updates metadata on the given HypervisorConnection.

Syntax

Set-HypHypervisorConnectionMetadata [-HypervisorConnectionUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHypervisorConnectionMetadata [-HypervisorConnectionUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHypervisorConnectionMetadata [-HypervisorConnectionName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHypervisorConnectionMetadata [-HypervisorConnectionName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHypervisorConnectionMetadata [-InputObject] <HypervisorConnection[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypHypervisorConnectionMetadata [-InputObject] <HypervisorConnection[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given HypervisorConnection objects.

Related topics

Add-HypHypervisorConnectionMetadata

Remove-HypHypervisorConnectionMetadata

Parameters

-HypervisorConnectionUid<Guid>

Id of the HypervisorConnection

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-HypervisorConnectionName<String>

Name of the HypervisorConnection

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<HypervisorConnection[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the HypervisorConnection specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-HypHypervisorConnectionMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-HypHypervisorConnectionMetadata -HypervisorConnectionUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

    Key                            Value
    ---                            -----
    property                           value
```

Add metadata with a name of 'property' and a value of 'value' to the HypervisorConnection with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-HypServiceMetadata

Sep 10, 2014

Adds or updates metadata on the given Service.

Syntax

Set-HypServiceMetadata [-ServiceHostId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypServiceMetadata [-InputObject] <Service[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Allows you to store additional custom data against given Service objects.

Related topics

Remove-HypServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Service specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-HypServiceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-HypServiceMetadata -ServiceHostId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Service with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-HypVolumeServiceConfiguration

Sep 10, 2014

Applies a change to one of the VolumeServiceConfiguration instances in the site.

Syntax

```
Set-HypVolumeServiceConfiguration -VolumeWorkerPackageUri <String> -ConnectionType <String> -VolumeServiceConfigurationName <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-HypVolumeServiceConfiguration -RegionName <String> -BaseLinuxTemplateId <String> -ConnectionType <String> -VolumeServiceConfigurationName <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Volume service configurations are used to control how cloud-based host connections behave when provisioning machines. They contain two pieces of information. The first is a per-region specification of the cloud template that provides the standard Linux operating system for the cloud. The second is the specification of a URL from which the Citrix Volume Worker software can be installed (not all cloud connections make use of this URL, but they all make use of the template map).

Each cmdlet invocation can be used to either change the volume worker URL, or to modify (or add) an entry in the Linux template map. These two operations are supported by parameter sets. To change both properties, you must invoke the cmdlet twice.

Related topics

Get-HypVolumeServiceConfiguration

Parameters

-ConnectionType<String>

Specifies the cloud connection type, such as "AWS" or "CloudPlatform".

Required?	true
Default Value	
Accept Pipeline Input?	false

-VolumeServiceConfigurationName<String>

Specifies the name of the configuration you want to modify. This parameter is used alongside the ConnectionType to specify a single configuration set unambiguously. There can be only one named configuration per connection type. In a newly-configured site, there will be exactly one configuration set called "SiteDefault" for each of CloudPlatform and AWS.

Required?	true
Default Value	
Accept Pipeline Input?	false

-VolumeWorkerPackageUri<String>

Specifies a (new) URI for the volume worker package.

Required?	true
Default Value	
Accept Pipeline Input?	false

-RegionName<String>

Specifies the cloud region in which the Linux template resides. This parameter is used only when passing the BaseLinuxTemplateId parameter. The format of the string is cloud-specific. For example, for an AWS-based cloud, it would be a region identifier such as "us-east-1".

Required?	true
Default Value	
Accept Pipeline Input?	false

-BaseLinuxTemplateId<String>

Specifies a change to the standard Linux template that should be used in the cloud. When passing this parameter, you must also specify the RegionName parameter to indicate the region in which

this template resides. The format of the string is cloud-specific. For example, for an AWS-based cloud, it would be an AMI identifier such as "ami-1234abcd".

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Host.Sdk.VolumeServiceConfiguration

This cmdlet returns the updated VolumeServiceConfiguration object.

Examples

---------- EXAMPLE 1 ----------

C:\PS>Set-HypVolumeServiceConfiguration -VolumeServiceConfigurationName SiteDefault -ConnectionType CloudPlatform -RegionName Region1 -BaseLinuxTemplateId 988
This command specifies a Linux template that should be used by default for CloudPlatform connections.

---------- EXAMPLE 2 ----------

C:\PS>Set-HypVolumeServiceConfiguration -VolumeServiceConfigurationName SiteDefault -ConnectionType CloudPlatform -VolumeWorkerPackageUri "http://cloudadmin.ne
This command specifies a worker package download URL that should be used by default for CloudPlatform connections.

Start-HypVM

Sep 10, 2014

Starts a VM.

Syntax

```
Start-HypVM [-LiteralPath] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

This command provides a mechanism to start a VM.

Related topics

Parameters

-LiteralPath<String>

Specifies the path within a hosting unit provider to the virtual machine item to start. The path specified must be in one of the following formats: <drive>:\Connections\<Connection Name>\<Item Path of VM object> or <drive>:\Connections\{<connection Uid>\<Item Path of VM object>} or <drive>:\HostingUnits\<HostingUnit Name>\<Item Path of VM object> or <drive>:\HostingUnits\{<hostingUnit Uid>\<Item Path of VM object>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path.

Return Values

System.void.

Notes

In the case of failure, the following errors can result.

Error Codes

InputHypervisorItemPathInvalid

The path provided is not to an item in a sub-directory of a connection item or a hosting unit item.

InvalidHypervisorItemPath

No item exists with the specified path.

InvalidHypervisorItem

The item specified by the path exists, but is not a VM Item.

HypervisorInMaintenanceMode

The hypervisor is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Start-HypVM -LiteralPath XDHyp:\Connections\MyConnection\MyVm.vm
```

This command starts a VM called 'MyVm.vm' within a hypervisor connection called 'MyConnection'.

Stop-HypVM

Sep 10, 2014

Stops a VM by issuing a Shutdown request

Syntax

```
Stop-HypVM [-LiteralPath] <String> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to change the power state of a VM from running to stopped.

Related topics

Parameters

-LiteralPath<String>

Specifies the path within a hosting unit provider to the virtual machine item to stop. The path specified must be in one of the following formats: <drive>:\Connections\<Connection Name>\<Item Path of VM object> or <drive>:\Connections\{<connection Uid>\<Item Path of VM object>} or <drive>:\HostingUnits\<HostingUnit Name>\<Item Path of VM object> or <drive>:\HostingUnits\{<hostingUnit Uid>\<Item Path of VM object>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in will connect to. This can be provided as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Input Type

System.string You can pipe a string that contains a path.

Return Values

System.void.

Notes

In the case of failure, the following errors can result.

Error Codes

InputHypervisorItemPathInvalid

The path provided is not to an item in a sub-directory of a connection item or a hosting unit item.

InvalidHypervisorItemPath

No item exists with the specified path.

InvalidHypervisorItem

The item specified by the path exists, but is not a VM Item.

HypervisorInMaintenanceMode

The hypervisor is in maintenance mode.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS>Stop-HypVM -LiteralPath XDHyp:\Connections\MyConnection\MyVm.vm
```

This command stops a VM called 'MyVm.vm' within a hypervisor connection called 'MyConnection'.

Test-HypDBConnection

Sep 10, 2014

Tests a database connection for the Host Service.

Syntax

```
Test-HypDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Tests a connection to the database in which the Host Service can store its state. The service will attempt to connect to the database without affecting the current connection to the database.

You do not have to clear the connection to use this command.

Related topics

Get-HypServiceStatus

Get-HypDBConnection

Set-HypDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the Host Service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-HypDBConnection command returns an object containing the status of the Host Service if the connection string of the specified data store were to be set to the string being tested, together with extra diagnostics information for the specified connection string.

DBRejectedConnection

The database rejected the logon attempt from the Host Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Host Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Host Service currently in use is incompatible with the version of the Host Service schema on the database. Upgrade the Host Service to a more recent version.

DBOlderVersionThanService

The version of the Host Service schema on the database is incompatible with the version of the Host Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Set-HypDBConnection command would succeed if it were executed with the supplied connection string.

Failed

The Host Service has failed.

Unknown

The status of the Host Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Test-HypDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Tests a database connection string for the Host Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Test-HypDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Tests an invalid database connection string for the Host Service.

Test-HypHostingUnitNameAvailable

Sep 10, 2014

Checks to ensure that the proposed name for a hosting unit is unused.

Syntax

```
Test-HypHostingUnitNameAvailable -HostingUnitName <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Use this command to check that the proposed name for a hosting unit is unused. This check is done without regard for scoping of the existing hosting unit, so the names of inaccessible hosting units are also checked.

Related topics

New-Item

Rename-Item

Parameters

-HostingUnitName<String[]>

The name or names of the hosting units(s) to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

object[]

An array of PSObjects which pair the name and availability of the name

Notes

In the case of failure, the following errors can result.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
Test-HypHostingUnitNameAvailable -HostingUnitName $NewHostingUnitName
```

This tests whether the value of $NewHostingUnitName is unique or not, and can be used to create a new hosting unit or rename an existing one without failing. True is returned if the name is unique.

Test-HypHypervisorConnectionNameAvailable

Sep 10, 2014

Checks to ensure that the proposed name for a hypervisor connection is unused.

Syntax

Test-HypHypervisorConnectionNameAvailable -HypervisorConnectionName <String[]> [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Use this command to check that the proposed name for a hypervisor connection is unused. This check is done without regard for scoping of the existing hypervisor connection, so the names of inaccessible hypervisor connection are also checked.

Related topics

New-Item

Rename-Item

Parameters

-HypervisorConnectionName<String[]>

The name or names of the hypervisor connection(s) to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

object[]

An array of PSObjects which pair the name and availability of the name

Notes

In the case of failure, the following errors can result.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
Test-HypHypervisorConnectionNameAvailable -HypervisorConnectionName $NewConnectionName
```

This tests whether the value of $NewConnectionName is unique or not, and can be used to create a new hypervisor connection or rename an existing one. True is returned if the name is unique.

Update-HypHypervisorConnection

Sep 10, 2014

Requests the host service to update the connection properties that depend on the version of hypervisor in use.

Syntax

```
Update-HypHypervisorConnection [-LiteralPath] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this command to update the version-specific properties of a hypervisor connection, after an upgrade to the hypervisor system which may provide new capabilities.

Related topics

Parameters

-LiteralPath<String>

Specifies the path within a Host Service provider to the hypervisor connection item to be updated. The path specified must be in one of the following formats; <drive>:\Connections\<HypervisorConnectionName> or <drive>:\Connections\{HypervisorConnection Uid>}

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in will connect to. This can be provided as a

host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value will become the default.
Accept Pipeline Input?	false

Notes

In the case of failure, the following errors can result.

Error Codes

InvalidPath

The path provided is not in the required format.

HypervisorInMaintenanceMode

The hypervisor is in maintenance mode and cannot be updated.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Update-HypHypervisorConnection -LiteralPath xdhyp:\connections\Connection1
```

This command requests that the properties of Connection1 be updated to match the current capabilities of the hypervisor.

Citrix.MachineCreation.Admin.V2

Sep 10, 2014

Overview

Name	Description
ProvMachineCreationSnapin	The Machine Creation Service PowerShell snap-in provides administrative
Prov Filtering	Describes the common filtering options for XenDesktop cmdlets.
providers	Describes how Windows PowerShell providers provide access to data and

Cmdlets

Name	Description
Add-ProvSchemeControllerAddress	Adds a list of host names (as DNS addresses) to a provisioning scheme.
Add-ProvSchemeMetadata	Adds metadata on the given ProvisioningScheme.
Add-ProvSchemeScope	Add the specified ProvisioningScheme(s) to the given scope(s).
Add-ProvTaskMetadata	Adds metadata on the given Task.
Get-ProvDBConnection	Gets the database string for the specified data store used by the MachineCreation Service.
Get-ProvDBSchema	Gets a script that creates the MachineCreation Service database schema for the specified data store.
Get-ProvDBVersionChangeScript	Gets a script that updates the MachineCreation Service database schema.
Get-ProvInstalledDBVersion	Gets a list of all available database schema versions for the MachineCreation Service.
Get-ProvObjectReference	Returns the number of local objects holding references to objects from other services.
Get-ProvScheme	Gets the list of provisioning schemes.
Get-ProvSchemeMasterVMImageHistory	Gets the list of master VM snapshots that have been used to provide hard disks to provisioning schemes.

Name	Description
Get-ProvScopedObject	Gets the details of the scoped objects for the MachineCreation Service.
Get-ProvService	Gets the service record entries for the MachineCreation Service.
Get-ProvServiceAddedCapability	Gets any added capabilities for the MachineCreation Service on the controller.
Get-ProvServiceConfigurationData	Gets configuration data for the service.
Get-ProvServiceInstance	Gets the service instance entries for the MachineCreation Service.
Get-ProvServiceStatus	Gets the current status of the MachineCreation Service on the controller.
Get-ProvTask	Gets the task history for the MachineCreation Service.
Get-ProvVM	Gets the VMs that were created using Citrix XenDesktop Machine Creation Services.
Lock-ProvVM	Locks a VM.
New-ProvScheme	Creates a new provisioning scheme.
New-ProvVM	Creates a new virtual machine.
Publish-ProvMasterVmImage	Update the master image associated with the provisioning scheme.
Remove-ProvScheme	Removes a provisioning scheme
Remove-ProvSchemeControllerAddress	Removes metadata from a provisioning scheme.
Remove-ProvSchemeMasterVMImageHistory	Removes the history of provisioning scheme master image VMs.
Remove-ProvSchemeMetadata	Removes metadata from the given ProvisioningScheme.
Remove-ProvSchemeScope	Remove the specified ProvisioningScheme(s) from the given scope(s).
Remove-ProvServiceConfigurationData	Removes configuration data from the service.
Remove-ProvServiceMetadata	Removes metadata from the given Service.

Name	Description
Remove-ProvTask	Removes from the database completed tasks for the MachineCreation Service.
Remove-ProvTaskMetadata	Removes metadata from the given Task.
Remove-ProvVM	Removes virtual machines.
Rename-ProvScheme	Renames a provisioning scheme.
Reset-ProvServiceGroupMembership	Reloads the access permissions and configuration service locations for the MachineCreation Service.
Set-ProvDBConnection	Configures a database connection for the MachineCreation Service.
Set-ProvScheme	Changes the parameter values for a provisioning scheme.
Set-ProvSchemeMetadata	Adds or updates metadata on the given ProvisioningScheme.
Set-ProvServiceConfigurationData	Sets the value for the given key in the service configuration data.
Set-ProvServiceMetadata	Adds or updates metadata on the given Service.
Set-ProvTaskMetadata	Adds or updates metadata on the given Task.
Stop-ProvTask	Stops currently running MachineCreation Service tasks.
Switch-ProvTask	Moves all MachineCreation Service tasks from the current execution host to another.
Test-ProvDBConnection	Tests a database connection for the MachineCreation Service.
Test-ProvSchemeNameAvailable	Checks to ensure that the proposed name for a provisioning scheme is unused.
Unlock-ProvScheme	Unlocks a Provisioning Scheme.
Unlock-ProvVM	Unlocks a VM.

about_ProvMachineCreationSnapin

Sep 10, 2014

TOPIC

about_ProvMachineCreationSnapin

SHORT DESCRIPTION

The Machine Creation Service PowerShell snap-in provides administrative functions for the Machine Creation Service.

COMMAND PREFIX

All commands in this snap-in have 'Prov' in their name.

LONG DESCRIPTION

The Machine Creation Service PowerShell snap-in enables both local and remote administration of the Machine Creation Service. It provides facilities to create virtual machines and manage the associated disk images.

The snap-in provides two main entities:

Provisioning Scheme

> Specifies details of new virtual machines created by the Machine Creation Service. Provisioning schemes define the following information.
>
> Hosting Unit
> Provides details of the hypervisor and storage on which new virtual machines will be created. Stored and maintained by the Host Service and PowerShell snap-in.
>
> Identity Pool
> Lists the Active Directory computer accounts available for use by new virtual machines. Stored and maintained by the Active Directory Identity Service and PowerShell snap-in.
>
> Master Image
> Specifies the disk image that will be used for new virtual machines. Accessed through the hosting provider in the Host Service snap-in.

Provisioned VM

> Defines the virtual machines created by the Machine Creation Services. These virtual machines are associated with the provisioning scheme from which they were created.

The processes of creating provisioning schemes and new virtual machines can take a significant amount of time to complete. For this reason, these long-running tasks can be run asynchronously so that other commands are accessible while the processes are running. Note, however, that only one long-running task can operate on a provisioning scheme at any one time. The processes are monitored using the Get-ProvTask command. For more information, see the help for Get-ProvTask.

about_Prov_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more
are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```

retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

```
Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }
```

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

```
A120901
B220000
...
```

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

about_providers

Sep 10, 2014

TOPIC

about_Providers

SHORT DESCRIPTION

Describes how Windows PowerShell providers provide access to data and components that would not otherwise be easily accessible at the command line. The data is presented in a consistent format that resembles a file system drive.

LONG DESCRIPTION

Windows PowerShell providers are Microsoft .NET Framework-based programs that make the data in a specialized data store available in Windows PowerShell so that you can view and manage it.

The data that a provider exposes appears in a drive, and you access the data in a path like you would on a hard disk drive. You can use any of the built-in cmdlets that the provider supports to manage the data in the provider drive. And, you can use custom cmdlets that are designed especially for the data.

The providers can also add dynamic parameters to the built-in cmdlets. These are parameters that are available only when you use the cmdlet with the provider data.

BUILT-IN PROVIDERS

Windows PowerShell includes a set of built-in providers that you can use to access the different types of data stores.

Provider Drive Data store -------- ----- ---------- Alias Alias: Windows PowerShell aliases

Certificate Cert: x509 certificates for digital signatures

Environment Env: Windows environment variables

FileSystem * File system drives, directories, and files

Function Function: Windows PowerShell functions

Registry HKLM:, HKCU Windows registry

Variable Variable: Windows PowerShell variables

WS-Management WSMan WS-Management configuration information

* The FileSystem drives vary on each system.

You can also create your own Windows PowerShell providers, and you can install providers that others develop. To list the providers that are available in your session, type:

```
get-psprovider
```

INSTALLING AND REMOVING PROVIDERS

Windows PowerShell providers are delivered to you in Windows PowerShell snap-ins, which are .NET Framework-based programs that are compiled into .dll files. The snap-ins can include providers and cmdlets.

Before you use the provider features, you have to install the snap-in and then add it to your Windows PowerShell session. For more information, see about_PsSnapins.

You cannot uninstall a provider, although you can remove the Windows PowerShell snap-in for the provider from the current session. If you do, you will remove all the contents of the snap-in, including its cmdlets.

To remove a provider from the current session, use the Remove-PsSnapin cmdlet. This cmdlet does not uninstall the provider, but it makes the provider unavailable in the session.

You can also use the Remove-PsDrive cmdlet to remove any drive from the current session. This data on the drive is not affected, but the drive is no longer available in that session.

VIEWING PROVIDERS

To view the Windows PowerShell providers on your computer, type:

```
get-psprovider
```

The output lists the built-in providers and the providers that you added to the session.

THE PROVIDER CMDLETS

The following cmdlets are designed to work with the data exposed by any provider. You can use the same cmdlets in the same way to manage the different types of data that providers expose. After you learn to manage the data of one provider, you can use the same procedures with the data from any provider.

For example, the New-Item cmdlet creates a new item. In the C: drive that is supported by the FileSystem provider, you can use New-Item to create a new file or folder. In the drives that are supported by the Registry provider, you can use New-Item to create a new registry key. In the Alias: drive, you can use New-Item to create a new alias.

For detailed information about any of the following cmdlets, type:

```
get-help <cmdlet-name> -detailed
```

CHILDITEM CMDLETS

```
Get-ChildItem
```

CONTENT CMDLETS

```
Add-Content
```

Clear-Content
Get-Content
Set-Content

ITEM CMDLETS

Clear-Item
Copy-Item
Get-Item
Invoke-Item
Move-Item
New-Item
Remove-Item
Rename-Item
Set-Item

ITEMPROPERTY CMDLETS

Clear-ItemProperty
Copy-ItemProperty
Get-ItemProperty
Move-ItemProperty
New-ItemProperty
Remove-ItemProperty
Rename-ItemProperty
Set-ItemProperty

LOCATION CMDLETS

Get-Location
Pop-Location
Push-Location
Set-Location

PATH CMDLETS

Join-Path
Convert-Path
Split-Path
Resolve-Path
Test-Path

PSDRIVE CMDLETS

```
Get-PSDrive
New-PSDrive
Remove-PSDrive
```

PSPROVIDER CMDLETS

```
Get-PSProvider
```

VIEWING PROVIDER DATA

The primary benefit of a provider is that it exposes its data in a familiar and consistent way. The model for data presentation is a file system drive.

To use data that the provider exposes, you view it, move through it, and change it as though it were data on a hard drive. Therefore, the most important information about a provider is the name of the drive that it supports.

The drive is listed in the default display of the Get-PsProvider cmdlet, but you can get information about the provider drive by using the Get-PsDrive cmdlet. For example, to get all the properties of the Function: drive, type:

```
get-psdrive Function | format-list *
```

You can view and move through the data in a provider drive just as you would on a file system drive.

To view the contents of a provider drive, use the Get-Item or Get-ChildItem cmdlets. Type the drive name followed by a colon (:). For example, to view the contents of the Alias: drive, type:

```
get-item alias:
```

You can view and manage the data in any drive from another drive by including the drive name in the path. For example, to view the HKLM\Software registry key in the HKLM: drive from another drive, type:

```
get-childitem hklm:\software
```

To open the drive, use the Set-Location cmdlet. Remember the colon when you specify the drive path. For example, to change your location to the root directory of the Cert: drive, type:

```
set-location cert:
```

Then, to view the contents of the Cert: drive, type:

```
get-childitem
```

MOVING THROUGH HIERARCHICAL DATA

You can move through a provider drive just as you would a hard disk drive. If the data is arranged in a hierarchy of items within items, use a backslash (\) to indicate a child item. Use the following format:

```
drive:\location\child-location\...
```

For example, to change your location to the HKLM\Software registry key, type a Set-Location command, such as:

```
set-location hklm:\software
```

You can also use relative references to locations. A dot (.) represents the current location. For example, if you are in the HKLM:\Software\Microsoft registry key, and you want to list the registry subkeys in the HKLM:\Software\Micrsoft\PowerShell key, type the following command:

```
get-childitem .\powershell
```

FINDING DYNAMIC PARAMETERS

Dynamic parameters are cmdlet parameters that are added to a cmdlet by a provider. These parameters are available only when the cmdlet is used with the provider that added them.

For example, the Cert: drive adds the CodeSigningCert parameter to the Get-Item and Get-ChildItem cmdlets. You can use this parameter only when you use Get-Item or Get-ChildItem in the Cert: drive.

For a list of the dynamic parameters that a provider supports, see the Help file for the provider. Type:

```
get-help <provider-name>
```

For example:

```
get-help certificate
```

LEARNING ABOUT PROVIDERS

Although all provider data appears in drives, and you use the same methods to move through them, the similarity stops there. The data stores that the provider exposes can be as varied as Active Directory locations and Microsoft Exchange Server mailboxes.

For information about individual Windows PowerShell providers, type:

```
get-help <ProviderName>
```

For example:

```
get-help registry
```

For a list of Help topics about the providers, type:

```
get-help * -category provider
```

SEE ALSO

about_Locations

about_Path_Syntax

Add-ProvSchemeControllerAddress

Sep 10, 2014

Adds a list of host names (as DNS addresses) to a provisioning scheme.

Syntax

```
Add-ProvSchemeControllerAddress [-ProvisioningSchemeName] <String> [-ControllerAddress] <String[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]

Add-ProvSchemeControllerAddress -ProvisioningSchemeUid <Guid> [-ControllerAddress] <String[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Provides the ability to associate controller hosts (and hence implicitly a set of brokers) with a specific provisioning scheme. This optional data is passed to the machines created by the Machine Creation Services, where it is used to associate the newly created machine with a broker. The list is returned along with the provisioning scheme that it is assigned to.

Related topics

Get-ProvScheme

Remove-ProvSchemeControllerAddress

Parameters

-ProvisioningSchemeName<String>

The name for the provisioning scheme that the list of addresses is to be added to.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeUid<Guid>

The unique identifier for the provisioning scheme that the list of addresses is to be added to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ControllerAddress<String[]>

Specifies the array of DNS names to be added to the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.MachineCreation.Sdk.ProvisioningScheme You can pipe an object containing a parameter called 'ProvisioningSchemeName' to Add-ProvSchemeControllerAddress.

Return Values

Citrix.MachineCreation.Sdk.ProvisioningScheme

Add-ProvSchemeControllerAddress returns the updated ProvisioningScheme object containing the union of the old and new controller address lists.

ProvisioningSchemeUid <Guid>

The unique identifier for the provisioning scheme.

ProvisioningSchemeName <string>

The name of the provisioning scheme.

CpuCount <int>

The number of processors that VMs will be created with when using this scheme.

MemoryMB <int>

The maximum amount of memory that VMs will be created with when using this scheme.

MasterImageVM <string>

The path within the hosting unit provider to the VM or snapshot of which the scheme is currently using a copy.

MasterImageVMDate <DateTime>

The date and time that the copy of the VM image was made for the scheme.

IdentityPoolUid <Guid>

The unique identifier of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

IdentityPoolName <string>

The name of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

HostingUnitUid <Guid>

The unique identifier of the hosting unit (from the Hosting Unit PowerShell snap-in) that the scheme will use.

HostingUnitName <string>

The name of the hosting unit (from the Hosting Unit PowerShell snap-in) that the scheme will use.

CleanOnBoot <Boolean>

Indicates whether or not the VMs created are to be reset to a clean state on each boot.

TaskId <Guid>

The identifier of any current task that is running for the provisioning scheme.

Metadata <Citrix.MachineCreation.Sdk.Metadata[]>

The metadata associated with this provisioning scheme.

ControllerAddress <string[]>

The DNS names of the controllers associated with this provisioning scheme for Quick Deploy purposes.

Notes

In the case of failure, the following errors can result.

Error Codes

ProvisioningSchemeNotFound

The specified provisioning scheme could not be located.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Add-ProvSchemeControllerAddress -ProvisioningSchemeUid "01a4a008-8ce8-4165-ba9c-cdf15a6b0501" -ControllerAddress (ddcA.citrix.com,ddcB.citrix.com,ddcC.citr

ProvisioningSchemeUid  : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
ProvisioningSchemeName : Scheme2
CpuCount               : 1
MemoryMB               : 1024
MasterImageVM          : Base.vm/Base.snapshot
MasterImageVMDate      : 17/05/2010 09:53:40
IdentityPoolUid        : 03743136-e43b-4a87-af74-ab71686b3c16
IdentityPoolName       : idPool1
HostingUnitUid         : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
HostingUnitName        : HostUnit1
CleanOnBoot            : True
TaskId                 : 00000000-0000-0000-0000-000000000000
Metadata               : {}
ControllerAddress      : {ddcA.citrix.com,ddcB.citrix.com,ddcC.citrix2.com}
```

Add a set of controllers to the provisioning scheme with the identifier "01a4a008-8ce8-4165-ba9c-cdf15a6b0501".

---------- EXAMPLE 2 ----------

```
C:\PS>Get-ProvScheme -ProvisioningSchemeName scheme1 | Add-ProvSchemeControllerAddress -ControllerAddress (ddcA.citrix.com,ddcB.citrix.com,ddcC.citrix2.com)

ProvisioningSchemeUid  : 7585f0de-192e-4847-a6d8-22713c3a2f42
ProvisioningSchemeName : Scheme1
CpuCount               : 1
MemoryMB               : 1024
MasterImageVM          : Base.vm/Base.snapshot
MasterImageVMDate      : 17/05/2010 09:53:40
IdentityPoolUid        : 03743136-e43b-4a87-af74-ab71686b3c16
IdentityPoolName       : idPool1
HostingUnitUid         : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
HostingUnitName        : HostUnit1
CleanOnBoot            : True
TaskId                 : 00000000-0000-0000-0000-000000000000
Metadata               : {}
ControllerAddress      : {ddcA.citrix.com,ddcB.citrix.com,ddcC.citrix2.com}
```

Add controller addresses to a provisioning scheme using a ProvisioningScheme object.

Add-ProvSchemeMetadata

Sep 10, 2014

Adds metadata on the given ProvisioningScheme.

Syntax

Add-ProvSchemeMetadata [-ProvisioningSchemeUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvSchemeMetadata [-ProvisioningSchemeUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvSchemeMetadata [-ProvisioningSchemeName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvSchemeMetadata [-ProvisioningSchemeName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvSchemeMetadata [-InputObject] <ProvisioningScheme[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvSchemeMetadata [-InputObject] <ProvisioningScheme[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given ProvisioningScheme objects. This cmdlet will not overwrite existing metadata on an object - use the Set-ProvSchemeMetadata cmdlet instead.

Related topics

Set-ProvSchemeMetadata

Remove-ProvSchemeMetadata

Parameters

-ProvisioningSchemeUid<Guid>

Id of the ProvisioningScheme

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ProvisioningSchemeName<String>

Name of the ProvisioningScheme

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<ProvisioningScheme[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the ProvisioningScheme specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.Metadata

Add-ProvSchemeMetadata returns an array of objects containing the new definition of the metadata.

\n Property <string>

\n Specifies the name of the property.

\n Value <string>

\n Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DuplicateObject

One of the specified metadata already exists.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-ProvSchemeMetadata -ProvisioningSchemeUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Property                       Value
        --------                      -----
        property                       value
```

Add metadata with a name of 'property' and a value of 'value' to the ProvisioningScheme with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Add-ProvSchemeScope

Sep 10, 2014

Add the specified ProvisioningScheme(s) to the given scope(s).

Syntax

```
Add-ProvSchemeScope [-Scope] <String[]> -InputObject <ProvisioningScheme[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvSchemeScope [-Scope] <String[]> -ProvisioningSchemeUid <Guid[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvSchemeScope [-Scope] <String[]> -ProvisioningSchemeName <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The AddProvSchemeScope cmdlet is used to associate one or more ProvisioningScheme objects with given scope(s).

There are multiple parameter sets for this cmdlet, allowing you to identify the ProvisioningScheme objects in different ways:

- ProvisioningScheme objects can be piped in or specified by the InputObject parameter

- The ProvisioningSchemeUid parameter specifies objects by ProvisioningSchemeUid

- The ProvisioningSchemeName parameter specifies objects by ProvisioningSchemeName (supports wildcards)

To add a ProvisioningScheme to a scope you need permission to change the scopes of the ProvisioningScheme and permission to add objects to all of the scopes you have specified.

If the ProvisioningScheme is already in a scope, that scope will be silently ignored.

Related topics

Remove-ProvSchemeScope

Get-ProvScopedObject

Parameters

-Scope<String[]>

Specifies the scopes to add the objects to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-InputObject<ProvisioningScheme[]>

Specifies the ProvisioningScheme objects to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ProvisioningSchemeUid<Guid[]>

Specifies the ProvisioningScheme objects to be added by ProvisioningSchemeUid.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ProvisioningSchemeName<String[]>

Specifies the ProvisioningScheme objects to be added by ProvisioningSchemeName.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

None

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

ScopeNotFound

One of the specified scopes was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command with the specified objects or scopes.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-ProvSchemeScope Finance -ProvisioningSchemeUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
```

Adds a single ProvisioningScheme to the 'Finance' scope.

---------- EXAMPLE 2 ----------

```
c:\PS>Add-ProvSchemeScope Finance,Marketing -ProvisioningSchemeUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
```

Adds a single ProvisioningScheme to the multiple scopes.

---------- EXAMPLE 3 ----------

```
c:\PS>Get-ProvScheme | Add-ProvSchemeScope Finance
```

Adds all visible ProvisioningScheme objects to the 'Finance' scope.

---------- EXAMPLE 4 ----------

```
c:\PS>Add-ProvSchemeScope Finance -ProvisioningSchemeName A*
```

Adds ProvisioningScheme objects with a name starting with an 'A' to the 'Finance' scope.

Add-ProvTaskMetadata

Sep 10, 2014

Adds metadata on the given Task.

Syntax

```
Add-ProvTaskMetadata [-TaskId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvTaskMetadata [-TaskId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvTaskMetadata [-InputObject] <Task[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Add-ProvTaskMetadata [-InputObject] <Task[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Use this cmdlet to store additional custom data against given Task objects. This cmdlet does not overwrite existing metadata on an object - use the Set-ProvTaskMetadata cmdlet instead.

Related topics

Set-ProvTaskMetadata

Remove-ProvTaskMetadata

Get-ProvTask

Stop-ProvTask

Remove-ProvTask

Switch-ProvTask

Parameters

-TaskId<Guid>

Id of the Task

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Task[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Task specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.Metadata

Add-ProvTaskMetadata returns an array of objects containing the new definition of the metadata.

Property <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can result.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DuplicateObject

One of the specified metadata already exists.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Add-ProvTaskMetadata -TaskId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Property                        Value
        --------                      -----
        property                        value
```

Add metadata with a name of 'property' and a value of 'value' to the Task with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Get-ProvDBConnection

Sep 10, 2014

Gets the database string for the specified data store used by the MachineCreation Service.

Syntax

```
Get-ProvDBConnection [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the database connection string for the specified data store.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

Related topics

Get-ProvServiceStatus

Set-ProvDBConnection

Test-ProvDBConnection

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

system.string

The database connection string configured for the MachineCreation Service.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the MachineCreation Service has not been specified.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvDBConnection

Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True
```

Get the database connection string for the MachineCreation Service.

Get-ProvDBSchema

Sep 10, 2014

Gets a script that creates the MachineCreation Service database schema for the specified data store.

Syntax

Get-ProvDBSchema [-DatabaseName <String>] [-ServiceGroupName <String>] [-ScriptType <ScriptTypes>] [-LocalDatabase] [-Sid <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets SQL scripts that can be used to create a new MachineCreation Service database schema, add a new MachineCreation Service to an existing site, remove a MachineCreation Service from a site, or create a database server logon for a MachineCreation Service. If no Sid parameter is provided, the scripts obtained relate to the currently selected MachineCreation Service instance, otherwise the scripts relate to MachineCreation Service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied. The current service instance is that on the local machine, or that explicitly specified by the last usage of the -AdminAddress parameter to a MachineCreation SDK cmdlet. The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured. The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SMDCMD mode'. The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to MachineCreation Service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to MachineCreation Service roles

If ScriptType is Evict, the returned script contains:

o Removal of MachineCreation Service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database. You do not need to configure a database before

using this command.

Related topics

Set-ProvDBConnection

Parameters

-DatabaseName<String>

Specifies the name of the database for which the schema will be generated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the MachineCreation services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<ScriptTypes>

Specifies the type of database script returned. Available script types are:

Database

Returns a full database script that can be used to create a database schema for the MachineCreation Service in a database instance that does not already contain a schema for this service. The DatabaseName and ServiceGroupName parameters must be specified to create a script of this type.

Instance

Returns a permissions script that can be used to add further MachineCreation services to an existing database instance that already contains the full MachineCreation service schema, associating the services to the Service Group. The Sid parameter can optionally be specified to create a script of this type.

Login

Returns a database logon script that can be used to add the required logon accounts to an existing database instance that contains the MachineCreation Service schema. This is used primarily when creating a mirrored database environment. The DatabaseName parameter must be specified to create a script of this type.

Evict

Returns a script that can be used to remove the specified MachineCreation Service from the database entirely. The DatabaseName and Sid parameters must be specified to create a script of this type.

Required?	false
Default Value	Database
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for MachineCreation services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Sid<String>

Specifies the SID of the controller on which the MachineCreation Service instance to remove from the database is running.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.string

A string containing the required SQL script for application to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvDBSchema -DatabaseName MyDB -ServiceGroupName  MyServiceGroup > c:\ProvSchema.sql
```

Get the full database schema for site data store of the MachineCreation Service and copy it to a file called 'c:\ProvSchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a MachineCreation Service site schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ProvDBSchema -DatabaseName MyDB -scriptType Login > c:\MachineCreationLogins.sql
```

Get the logon scripts for the MachineCreation Service.

Get-ProvDBVersionChangeScript

Sep 10, 2014

Gets a script that updates the MachineCreation Service database schema.

Syntax

```
Get-ProvDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a database script that can be used to upgrade or downgrade the site or secondary schema for the MachineCreation Service from the current schema version to a different version.

Related topics

Get-ProvInstalledDBVersion

Parameters

-DatabaseName<String>

Specifies the name of the database instance to which the update applies.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

Specifies the version of the database you want to update to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

A PSObject containing the required SQL script for application to a database.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any MachineCreation services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-ProvServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the MachineCreation Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $update = Get-ProvDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-ProvInstalledDBVersion

Sep 10, 2014

Gets a list of all available database schema versions for the MachineCreation Service.

Syntax

```
Get-ProvInstalledDBVersion [-Upgrade] [-Downgrade] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the current version of the MachineCreation Service database schema, if no flags are set, otherwise returns versions for which upgrade or downgrade scripts are available and have been stored in the database.

Related topics

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Version

The Get-ProvInstalledDbVersion command returns objects containing the new definition of the MachineCreation Service database schema version.

Major <Integer>

Minor <Integer>

Build <Integer>

Revision <Integer>

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the MachineCreation Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-ProvInstalledDBVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      6      0      0
```

Get the currently installed version of the MachineCreation Service database schema.

-------------------------- EXAMPLE 2 --------------------------

```
c:\PS>Get-ProvInstalledDBVersion -Upgrade

Major  Minor  Build  Revision
-----  -----  -----  --------
6      0      0      0
```

Get the versions of the MachineCreation Service database schema for which upgrade scripts are supplied.

Get-ProvObjectReference

Sep 10, 2014

Returns the number of local objects holding references to objects from other services.

Syntax

Get-ProvObjectReference [-HostingUnitUid <Guid[]>] [-IdentityPoolUid <Guid[]>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns for each hosting unit or identity pool GUID the number of references by provisioning schemes or by long running task. This check is done without regard for scoping of existing provisioning schemes, references by inaccessible schemes are also checked.

Related topics

Parameters

-HostingUnitUid<Guid[]>

The identifiers of the hosting units(s) to be tested.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-IdentityPoolUid<Guid[]>

The identifiers of the identity pool(s) to be tested.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

ObjectReferenceCount

An object which contain the input object identifier, its type, the type of referencing object and the number of references.

Notes

In the case of failure, the following errors can result.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
Get-ProvObjectReference -HostingUnitUid 5B66A060-85E1-4DBD-9D1B-BF79881D3BB1

Count        : 1
```

```
ObjectId    : 5b66a060-85e1-4dbd-9d1b-bf79881d3bb1
Source      : ProvisioningScheme
Target      : HostingUnit

Count       : 0
ObjectId    : 5b66a060-85e1-4dbd-9d1b-bf79881d3bb1
Source      : Task
Target      : HostingUnit
```

This checks a single hosting unit for objects that have references to them; in this case we only have a single provisioning scheme that relates to it.

Get-ProvScheme

Sep 10, 2014

Gets the list of provisioning schemes.

Syntax

Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Lets you retrieve the list of defined provisioning schemes.

Related topics

New-ProvScheme

Remove-ProvScheme

Add-ProvSchemeMetadata

Remove-ProvSchemeMetadata

Add-ProvSchemeControllerAddress

Remove-ProvSchemeControllerAddress

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningSchemeUid<Guid>

The unique identifier of the provisioning scheme.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ScopeId<Guid>

Gets only results with a scope matching the specified scope identifier.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScopeName<String>

Gets only results with a scope matching the specified scope name.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

See about_Prov_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

See about_Prov_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-Skip<Int32>

See about_Prov_Filtering for details.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

See about_Prov_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Filter<String>

See about_Prov_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. When a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.ProvisioningScheme

This object provides details of the provisioning scheme and contains the following information:

ProvisioningSchemeUid <Guid>

The unique identifier for the provisioning scheme.

ProvisioningSchemeName <string>

The name of the provisioning scheme.

CpuCount <int>

The number of processors that VMs will be created with when using this scheme.

MemoryMB <int>

The maximum amount of memory that VMs will be created with when using this scheme.

MasterImageVM <string>

The path within the hosting unit provider to the copy of the VM snapshot that the scheme uses.

MasterImageVMDate <DateTime>

The date and time that the copy was made of the VM snapshot used by the scheme.

IdentityPoolUid <Guid>

The unique identifier of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

IdentityPoolName <string>

The name of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

HostingUnitUid <Guid>

The unique identifier of the hosting unit (from the Hosting Unit PowerShell snap-in) that the scheme uses.

HostingUnitName <string>

The name of the hosting unit (from the Hosting Unit PowerShell snap-in) that the scheme uses.

CleanOnBoot <Boolean>

Indicates whether the VMs that are created will be reset to a clean state on each boot.

TaskId <Guid>

The identifier of any current task that is running for the provisioning scheme.

Metadata <Citrix.MachineCreation.Sdk.Metadata[]>

The metadata associated with this provisioning scheme.

ControllerAddress <string[]>

The DNS names of the controllers associated with this provisioning scheme for Quick Deploy purposes.

VMMetadata <char[]>

The opaque VM metadata block

UsePersonalVDiskStorage <bool>

True if the scheme will use personal vDisk storage.

PersonalVDiskDriveLetter <char>

The drive letter for the personal vDisk

PersonalVDiskDriveSize <int>

The size of the personal vDisk in GB

ProfileUsagePercentage <double>

The percentage of the personal vDisk to be used for profile data

DedicatedTenancy <bool>

Whether to use dedicated tenancy when creating machines in Cloud Hypervisors.

Notes

In the case of failure, the following errors can result.

Error Codes

PartialData

Only a subset of the available data was returned.

CouldNotQueryDatabase

The query to get the database was not defined.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

CommunicationError

An error occurred while communicating with the service.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-ProvScheme


ProvisioningSchemeUid  : 7585f0de-192e-4847-a6d8-22713c3a2f42
ProvisioningSchemeName : Scheme1
CpuCount               : 1
MemoryMB               : 1024
MasterImageVM          : /Base.vm/base.snapshot
MasterImageVMDate      : 17/05/2010 09:27:50
IdentityPoolUid        : 03743136-e43b-4a87-af74-ab71686b3c16
IdentityPoolName       : idPool1
HostingUnitUid         : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
HostingUnitName        : HostUnit1
CleanOnBoot            : True
TaskId                 : 00000000-0000-0000-0000-000000000000
Metadata               : {Department = Sales}
ControllerAddress      : {}
VMMetadata             : {0, 1, 0, 0...}

ProvisioningSchemeUid  : 43d82099-1fd7-4617-93f0-25b160813905
ProvisioningSchemeName : Scheme2
CpuCount               : 1
MemoryMB               : 1024
MasterImageVM          : /Base.vm/base.snapshot
MasterImageVMDate      : 17/05/2010 09:53:40
IdentityPoolUid        : 03743136-e43b-4a87-af74-ab71686b3c16
IdentityPoolName       : idPool1
HostingUnitUid         : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
HostingUnitName        : HostUnit1
CleanOnBoot            : True
TaskId                 : 00000000-0000-0000-0000-000000000000
Metadata               : {}
```

```
ControllerAddress     : {}
VMMetadata            : {0, 1, 0, 0...}
```
Returns all of the available provisioning schemes.

---------- EXAMPLE 2 ----------

```
C:\PS>Get-ProvScheme -ProvisioningSchemeName Scheme[0-1]


ProvisioningSchemeUid  : 7585f0de-192e-4847-a6d8-22713c3a2f42
ProvisioningSchemeName : Scheme1
CpuCount               : 1
MemoryMB               : 1024
MasterImageVM          : /Base.vm/base.snapshot
MasterImageVMDate      : 17/05/2010 09:27:50
IdentityPoolUid        : 03743136-e43b-4a87-af74-ab71686b3c16
IdentityPoolName       : idPool1
HostingUnitUid         : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
HostingUnitName        : HostUnit1
CleanOnBoot            : True
TaskId                 : 00000000-0000-0000-0000-000000000000
Metadata               : {}
ControllerAddress      : {}
VMMetadata             : {0, 1, 0, 0...}
```
Returns all of the provisioning schemes that have the name 'Scheme0' or 'Scheme1'.

Get-ProvSchemeMasterVMImageHistory

Sep 10, 2014

Gets the list of master VM snapshots that have been used to provide hard disks to provisioning schemes.

Syntax

Get-ProvSchemeMasterVMImageHistory [-ProvisioningSchemeName <String>] [-ProvisioningSchemeUid <Guid>] [-MasterImageVM <String>] [-VMImageHistoryUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to discover the master VM snapshots that have been used previously to provide the hard disk image for provisioning schemes. This information includes the date and time when the image was introduced. This information can be used to roll back a provisioning scheme to a previous image.

Related topics

Publish-ProvMasterVMImage

Remove-ProvSchemeMasterVMImageHistory

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningSchemeUid<Guid>

The unique identifier of the provisioning scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-MasterImageVM<String>

The path to the snapshot item in the hosting unit PowerShell provider.

Required?	false
Default Value	
Accept Pipeline Input?	false

-VMImageHistoryUid<Guid>

The unique identifier for the Image History item.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

See about_Prov_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

See about_Prov_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-Skip<Int32>

See about_Prov_Filtering for details.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

See about_Prov_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Filter<String>

See about_Prov_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.VMImage

The object that represents a master VM history. This contains the following parameters:

VMImageHistoryUid <Guid>

The unique identifier for the History item.

ProvisioningSchemeUid <Guid>

The unique identifier for the provisioning scheme that the VM was used for.

ProvisioningSchemeName <string>

The name of the provisioning scheme that the VM was used for.

MasterImageVM <string>

The path to the Snapshot item that was used as the master VM image.

Date <DateTime>

The date and time that the VM or snapshot was used in the provisioning scheme.

Notes

In the case of failure, the following errors can result.

Error Codes

PartialData

Only a subset of the available data was returned.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

CouldNotQueryDatabase

The query required to get the database was not defined.

CommunicationError

An error occurred while communicating with the service.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

C:\PS>Get-ProvSchemeMasterVMImageHistory

```
VMImageHistoryUid      : 3cba3a75-89cd-4868-989b-27feb378fec5
ProvisioningSchemeUid  : 7585f0de-192e-4847-a6d8-22713c3a2f42
ProvisioningSchemeName : MyScheme
MasterImageVM          : /Base.vm/base.snapshot
Date                   : 17/05/2010 09:27:50
```

Gets all the hard disk images that have been used across all provisioning schemes.

-------------------------- EXAMPLE 2 --------------------------

C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningScheme MyScheme -masterImageVM "/BaseXp.vm/update1.snapshot" | Publish-ProvMasterVmImage

Roll back the provisioning scheme to use the hard disk from the update1.snapshot for the provisioning scheme called "MyScheme".

Get-ProvScopedObject

Sep 10, 2014

Gets the details of the scoped objects for the MachineCreation Service.

Syntax

Get-ProvScopedObject [-ScopeId <Guid>] [-ScopeName <String>] [-ObjectType <ScopedObjectType>] [-ObjectId <String>] [-ObjectName <String>] [-Description <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns a list of directly scoped objects including the names and identifiers of both the scope and object as well as the object description for display purposes.

There will be at least one result for every directly scoped object. When an object is associated with multiple scopes the output contains one result per scope duplicating the object details.

No records are returned for the All scope, though if an object is not in any scope a result with a null ScopeId and ScopeName will be returned.

Related topics

Parameters

-ScopeId<Guid>

Gets scoped object entries for the given scope identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ScopeName<String>

Gets scoped object entries with the given scope name.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ObjectType<ScopedObjectType>

Gets scoped object entries for objects of the given type.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ObjectId<String>

Gets scoped object entries for objects with the specified object identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ObjectName<String>

Gets scoped object entries for objects with the specified object identifier.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-Description<String>

Gets scoped object entries for objects with the specified description.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Prov_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Prov_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.ScopedObject

The Get-ProvScopedObject command returns an object containing the following properties:

ScopeId <Guid?>

Specifies the unique identifier of the scope.

ScopeName <String>

Specifies the display name of the scope.

ObjectType <ScopedObjectType>

Type of the object this entry relates to.

ObjectId <String>

Unique identifier of the object.

ObjectName <String>

Display name of the object

Description <String>

Description of the object (possibly $null if the object type does not have a description).

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvScopedObject -ObjectType Scheme

ScopeId    : eff6f464-f1ee-4442-add3-99982e0cec01
ScopeName  : Sales
ObjectType : Scheme
ObjectId   : cd4174ee-9e4b-4e57-b126-9dbf757fe493
ObjectName : MyExampleScheme
Description : Test scheme

ScopeId    : 304e0fa7-d390-47f0-a94f-7e956a324c41
ScopeName  : Finance
ObjectType : Scheme
ObjectId   : cd4174ee-9e4b-4e57-b126-9dbf757fe493
ObjectName : MyExampleScheme
Description : Test scheme

ScopeId    :
ScopeName  :
ObjectType : Scheme
ObjectId   : 5062e46b-71bc-4ac9-901a-30fe6797e2f6
ObjectName : AnotherScheme
Description : Another scheme in no scopes
```

Gets all of the scoped objects with type Scheme. The example output shows a scheme object (MyExampleScheme) in two scopes Sales and Finance, and another scheme (AnotherScheme) that is not in any scope. The ScopeId and ScopeName values returned are null in the final record.

Get-ProvService

Sep 10, 2014

Gets the service record entries for the MachineCreation Service.

Syntax

Get-ProvService [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns instances of the MachineCreation Service that the service publishes. The service records contain account security identifier information that can be used to remove each service from the database.

A database connection for the service is required to use this command.

Related topics

Parameters

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Prov_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Prov_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.Service

The Get-ProvServiceInstance command returns an object containing the following properties.

Uid <Integer>

Specifies the unique identifier for the service in the group. The unique identifier is an index number.

ServiceHostId <Guid>

Specifies the unique identifier for the service instance.

DNSName <String>

Specifies the domain name of the host on which the service runs.

MachineName <String>

Specifies the short name of the host on which the service runs.

CurrentState <Citrix.Fma.Sdk.ServiceCore.ServiceState>

Specifies whether the service is running, started but inactive, stopped, or failed.

LastStartTime <DateTime>

Specifies the date and time at which the service was last restarted.

LastActivityTime <DateTime>

Specifies the date and time at which the service was last stopped or restarted.

OSType

Specifies the operating system installed on the host on which the service runs.

OSVersion

Specifies the version of the operating system installed on the host on which the service runs.

ServiceVersion

Specifies the version number of the service instance. The version number is a string that reflects the full build version of the service.

DatabaseUserName <string>

Specifies for the service instance the Active Directory account name with permissions to access the database. This will be either the machine account or, if the database is running on a controller, the NetworkService account.

Sid <string>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

ActiveSiteServices <string[]>

Specifies the names of active site services currently running in the service. Site services are components that perform long-running background processing in some services. This field is empty for services that do not contain site services.

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-ProvService

Uid             : 1
ServiceHostId     : aef6f464-f1ee-4042-a523-66982e0cecd0
DNSName           : MyServer.company.com
MachineName       : MYSERVER
CurrentState      : On
LastStartTime     : 04/04/2011 15:25:38
LastActivityTime  : 04/04/2011 15:33:39
OSType            : Win32NT
OSVersion         : 6.1.7600.0
ServiceVersion    : 5.1.0.0
DatabaseUserName  : NT AUTHORITY\NETWORK SERVICE
SID               : S-1-5-21-2316621082-1546847349-2782505528-1165
ActiveSiteServices : {MySiteService1, MySiteService2...}
```

Get all the instances of the MachineCreation Service running in the current service group.

Get-ProvServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the MachineCreation Service on the controller.

Syntax

```
Get-ProvServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the MachineCreation Service on the controller to be detected.

You do not need to configure a database connection before using this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvServiceAddedCapability
```

Get the added capabilities of the MachineCreation Service.

Get-ProvServiceConfigurationData

Sep 10, 2014

Gets configuration data for the service.

Syntax

Get-ProvServiceConfigurationData [-Name <String[]>] [-Value <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to determine the configuration parameters for the service

Related topics

Set-ProvServiceConfigurationData

Remove-ProvServiceConfigurationData

Parameters

-Name<String[]>

The Configuration data item Name .

Required?	false
Default Value	
Accept Pipeline Input?	false

-Value<String[]>

The Configuration data item value.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Prov_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Prov_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.ServiceConfigurationData

This object provides details of the configuration data and contains the following information:

Name <string>

The Name for the configuration item.

Value <string>

The value for the configuration item.

Notes

In the case of failure the following errors can be produced.

Error Codes

PartialData

Only a subset of the available data was returned.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-ProvConfiguratuionData

Name            : DeltaDiskDelete.timeDelay
Value           : 10
```

Get the Configuration data for the service.

Get-ProvServiceInstance

Sep 10, 2014

Gets the service instance entries for the MachineCreation Service.

Syntax

```
Get-ProvServiceInstance [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns service interfaces published by the instance of the MachineCreation Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.ServiceInstance

The Get-ProvServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a

central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

Specifies the service instance type. For this service, the service instance type is always Prov.

Address

Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

SDK - for PowerShell operations

InterService - for operations between different services

Peer - for communications between services of the same type

Metadata <Citrix.MachineCreation.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-ProvServiceInstance

Address          : http://MyServer.com:80/Citrix/MachineCreationService
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         :
MetadataMap      :
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName  : MyServiceGroup
ServiceGroupUid   : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType      : Prov
Version          : 1

Address          : http://MyServer.com:80/Citrix/MachineCreationService/IServiceApi
Binding          : wcf_HTTP_kerb
InterfaceType    : InterService
Metadata         :
MetadataMap      :
```



```
ServiceAccount     : ENG\MyAccount
ServiceAccountSid  : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName   : MyServiceGroup
ServiceGroupUid    : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType        : Prov
Version            : 1
```

Get all instances of the MachineCreation Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-ProvServiceStatus

Sep 10, 2014

Gets the current status of the MachineCreation Service on the controller.

Syntax

```
Get-ProvServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the MachineCreation Service on the controller to be monitored. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured.

Related topics

Set-ProvDBConnection

Test-ProvDBConnection

Get-ProvDBConnection

Get-ProvDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-ProvServiceStatus command returns an object containing the status of the MachineCreation Service together with extra diagnostics information.

DBUnconfigured

The MachineCreation Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the MachineCreation Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the MachineCreation Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the MachineCreation Service currently in use is incompatible with the version of the MachineCreation Service schema on the database. Upgrade the MachineCreation Service to a more recent version.

DBOlderVersionThanService

The version of the MachineCreation Service schema on the database is incompatible with the version of the MachineCreation Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The MachineCreation Service is running and is connected to a database containing a valid schema.

Failed

The MachineCreation Service has failed.

Unknown

(0) The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvServiceStatus

DBUnconfigured
```

Get the current status of the MachineCreation Service.

Get-ProvTask

Sep 10, 2014

Gets the task history for the MachineCreation Service.

Syntax

Get-ProvTask [[-TaskId] <Guid>] [-Type <JobType>] [-Active <Boolean>] [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns a list of tasks that have run or are currently running within the MachineCreation Service.

Related topics

Remove-ProvTask

Stop-ProvTask

Switch-ProvTask

Add-ProvTaskMetadata

Remove-ProvTaskMetadata

Parameters

-TaskId<Guid>

Specifies the task identifier to be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Type<JobType>

Specifies the type of task to be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Active<Boolean>

Specifies whether currently running tasks only or completed tasks only are returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Prov_Filtering for details.

Required?	false
Default Value	False

Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Prov_Filtering for details.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can result.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for

various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvTask -Active $false

TaskId               : cfe5b3a2-c471-443e-b05e-8658e672d10f
Type                 : MyTask
Host                 : NYSERVER
Status               : Finished
CurrentOperation     :
TaskProgress         : 100
TaskExpectedCompletion  : 10/10/2012 15:28:12
LastUpdateTime       : 10/10/2012 15:28:12
ActiveElapsedTime    : 56
DateFinished         : 10/10/2012 15:28:12
TerminatingError     :
...
```

Get all completed tasks for the MachineCreation Service.

All tasks will publish at least the fields listed above, plus more related to the particular task being performed.

Get-ProvVM

Sep 10, 2014

Gets the VMs that were created using Citrix XenDesktop Machine Creation Services.

Syntax

Get-ProvVM [[-ProvisioningSchemeName] <String>] [-ProvisioningSchemeUid <Guid>] [-VMName <String>] [-Locked <Boolean>] [-Tag <String>] [-OutOfDate] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to obtain a list of the VMs that were created using Machine Creation Services.

Related topics

New-ProvVM

Remove-ProvVM

Lock-ProvVM

Unlock-ProvVM

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ProvisioningSchemeUid<Guid>

The unique identifier of the provisioning scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-VMName<String>

The name of the VM in the hypervisor context.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Locked<Boolean>

Indicates whether only VMs that are marked as locked are returned or not (see Lock-ProvVM and Unlock-ProvVM for details).

Required?	false
Default Value	
Accept Pipeline Input?	false

-Tag<String>

The tag string that was associated with the VM when it was locked.

Required?	false
Default Value	
Accept Pipeline Input?	false

-OutOfDate<SwitchParameter>

Indicates that the image currently assigned to the VM is out of date. The image will be updated the next time the VM is restarted.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

See about_Prov_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

See about_Prov_Filtering for details.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-Skip<Int32>

See about_Prov_Filtering for details.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

See about_Prov_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Filter<String>

See about_Prov_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.ProvisionedVirtualMachine

The object has the following properties:

ADAccountSid <string>

The SID of the AD computer account that the VM is using.

ADAccountName <string>

The name of the AD computer account that the VM is using.

CpuCount <int>

The number of processors that the VM has been allocated.

CreationDate <DateTime>

The date and time that the VM was created.

Domain <string>

The Domain of the AD computer account that the VM is using.

ImageOutOfDate <Boolean>

Indicates if the image will be updated next time the VM is started.

Lock <Boolean>

Indicates whether the VM is locked or not.

MemoryMB <int>

The maximum amount of memory that VMs will be created with when using this scheme.

ProvisioningSchemeName <string>

The name of the provisioning scheme that the VM is part of.

ProvisioningSchemeUid <Guid>

The unique identifier for the provisioning scheme that the VM is part of.

Tag <string>

Provides the string associated with a locked VM.

VMId <string>

The identifier for the VM (hypervisor context).

VMName <string>

The name of the VM (hypervisor context).

AssignedImage <string>

The identifier (in the hypervisor) for the hard disk image that the VM is currently assigned.

BootedImage <string>

The identifier (in the hypervisor) for the hard disk image with which the VM is currently started.

HostingUnitUid <Guid>

The unique identifier for the hosting unit that was used to create the VM.

HypervisorConnectionUid <Guid>

The unique identifier of the hypervisor connection that was used to create the VM.

LastBootTime <DateTime>

The date and time of the last start of the VM.

OSDiskIndex <int>

The disk index at which the hard disk image, from which the VM is currently started, is attached (or [int]::MinValue for VMs inherited from versions of XenDesktop before 5.6)

PersonalVDiskIndex <int>

The disk index at which the personal vdisk is attached (defaults to [int]::MinValue for VMs without a personal vdisk)

PersonalVDiskStorage <string>

The identifier (in the hypervisor) for the storage on which the personal virtual disk image from which the VM is currently started is located. This is set only if the VM has a personal vDisk attached

StorageId <string>

The identifier (in the hypervisor) for the storage on which the hard disk image, from which the VM is currently started, is located.

Notes

In the case of failure, the following errors can result.

Error Codes

PartialData

Only a subset of the available data was returned.

CouldNotQueryDatabase

The query required to get the database was not defined.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

CommunicationError

An error occurred while communicating with the service.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-ProvVM -provisioningSchemeName MyScheme
```



```
ADAccountName         : MYDomain\computer2$
ADAccountSid          : S-1-5-21-3751941309-1176885247-1409628468-3179
CpuCount              : 1
CreationDate          : 17/05/2012 09:35:22
Domain                : steve.dum.local
ImageOutOfDate        : False
Lock                  : True
MemoryMB              : 512
ProvisioningSchemeName  : XenPS
ProvisioningSchemeUid   : 5135a865-ba49-4e5f-87f2-2d65ee7a4e51
Tag                   : Brokered
VMId                  : a830de93-ddc5-b763-dc1a-35580a31401c
VMName                : IP0051
AssignedImage         : 57fc60c3-eb9b-4d38-8646-0afceec85335
BootedImage           : 57fc60c3-eb9b-4d38-8646-0afceec85335
HostingUnitUid        : ea17840f-cf2d-4d80-94e0-3b752b32e0af
HypervisorConnectionUid : 99f9f826-31fc-4453-8ca0-9ba54306c3ac
IdentityDiskIndex     : 1
LastBootTime          : 17/05/2012 09:35:22
OSDiskIndex           : 0
PersonalVDiskIndex    : -2147483648
PersonalVDiskStorage  :
StorageId             : 33ad07a7-edd7-589b-716a-86cad4739f5e
```

Gets all the Virtual Machines that were provisioned into the Provisioning Scheme called 'MyScheme'.

---------- EXAMPLE 2 ----------

```
C:\PS>Get-ProvVM -Locked $true

ADAccountName         : MYDomain\computer1$
ADAccountSid          : S-1-5-21-3751941309-1176885247-1409628468-3178
CpuCount              : 1
CreationDate          : 17/05/2012 09:35:30
Domain                : steve.dum.local
ImageOutOfDate        : False
Lock                  : True
MemoryMB              : 512
ProvisioningSchemeName  : XenPS
ProvisioningSchemeUid   : 5135a865-ba49-4e5f-87f2-2d65ee7a4e51
Tag                   : Brokered
VMId                  : a830de93-ddc5-b763-dc1a-35580a31401c
VMName                : IP0051
AssignedImage         : 57fc60c3-eb9b-4d38-8646-0afceec85335
BootedImage           : 57fc60c3-eb9b-4d38-8646-0afceec85335
HostingUnitUid        : ea17840f-cf2d-4d80-94e0-3b752b32e0af
HypervisorConnectionUid : 99f9f826-31fc-4453-8ca0-9ba54306c3ac
IdentityDiskIndex     : 1
LastBootTime          : 17/05/2012 09:35:22
```

```
OSDiskIndex           : 0
PersonalVDiskIndex    : -2147483648
PersonalVDiskStorage  :
StorageId             : 33ad07a7-edd7-589b-716a-86cad4739f5e
```

Gets all the Virtual Machines that were locked, regardless of which Provisioning Scheme the VM is part of.

Lock-ProvVM

Sep 10, 2014

Locks a VM.

Syntax

Lock-ProvVM [-VMID] <String[]> -ProvisioningSchemeName <String> [-Tag <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Lock-ProvVM [-VMID] <String[]> -ProvisioningSchemeUid <Guid> [-Tag <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to 'lock' a virtual machine with a tag string. This stops other commands from being able to remove the virtual machine without unlocking the VM first. This is to enable consumers of the virtual machines to indicate that the VM is being used.

Related topics

UnLock-ProvVM

Get-ProvVM

Remove-ProvVM

Parameters

-VMID<String[]>

The virtual machine Id (hypervisor context).

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeName<String>

The name of the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeUid<Guid>

The unique identifier of the provisioning scheme.

Required?	true
Default Value	

Accept Pipeline Input?	false

-Tag<String>

The string to be held against the VM being locked.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.MachineCreation.Sdk.ProvisionedVirtualMachine You can pipe an object containing a parameter called 'VMId' and 'ProvisioningSchemeName' to Lock-ProvVM

Notes

In the case of failure, the following errors can result.

Error Codes

VMDoesNotExist

The specified VM cannot be located.

VMAlreadyLocked

The VM is already unlocked.

VMDoesNotExistForProvisioningScheme

The specified VM does exist in the hypervisor, but is not part of the specified provisioning scheme.

PermissionDenied

The user is not authorized to perform this operation

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Lock-ProvVM -provisioningSchemeName MyScheme -VMId  bc79802c-ba6e-8de8-99e9-4c35d7ad24b4 -Tag LockedString
```

Locks the VM with the Id 'bc79802c-ba6e-8de8-99e9-4c35d7ad24b4' in the provisioning scheme 'MyScheme' with the tag 'LockedString'.

---------- EXAMPLE 2 ----------

```
C:\PS>Get-ProvVM -provisioningSchemeName MyScheme | Lock-ProvVM -Tag LockedString
```

Locks all the VMs in the provisioning scheme 'MyScheme' with the tag 'LockedString'.

New-ProvScheme

Sep 10, 2014

Creates a new provisioning scheme.

Syntax

New-ProvScheme [-ProvisioningSchemeName] <String> -HostingUnitName <String> -IdentityPoolName <String> -MasterImageVM <String> [-VMCpuCount <Int32>] [-VMMemoryMB <Int32>] [-CleanOnBoot] [-UsePersonalVDiskStorage] [-Scope <String[]>] [-NoImagePreparation] [-NetworkMapping <Hashtable>] [-Metadata <Hashtable>] [-ServiceOffering <String>] [-SecurityGroup <String[]>] [-DedicatedTenancy] [-VhdTemplateSource <String>] [-VhdResultDestination <String>] [-AppScanResultsFile <String>] [-ResetAdministratorPasswords] [-RunAsynchronously] [-PurgeJobOnSuccess] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-ProvScheme [-ProvisioningSchemeName] <String> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> -MasterImageVM <String> [-VMCpuCount <Int32>] [-VMMemoryMB <Int32>] [-CleanOnBoot] [-UsePersonalVDiskStorage] [-Scope <String[]>] [-NoImagePreparation] [-NetworkMapping <Hashtable>] [-Metadata <Hashtable>] [-ServiceOffering <String>] [-SecurityGroup <String[]>] [-DedicatedTenancy] [-VhdTemplateSource <String>] [-VhdResultDestination <String>] [-AppScanResultsFile <String>] [-ResetAdministratorPasswords] [-RunAsynchronously] [-PurgeJobOnSuccess] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Lets you create a new provisioning scheme. The creation process makes a copy of the hard disk attached to a virtual machine snapshot and stores it in every storage location that the hosting unit referenced by the provisioning scheme defines. This is a long-running task and typically takes several minutes to complete (depending on the size of the hard disk that is being copied and the number of snapshots that the hard disk consists of).

A snapshot must be used rather than a VM, so that the content of the hard disk for the provisioning scheme can be easily determined.

As the snapshot is specified using a path into the Citrix Host Service Powershell Provider the Citrix Host Service Powershell snap-in must also be loaded for this cmdlet to be used.

This cmdlet requires information to be provided that is retrieved using other snap-ins that form part of the Citrix Machine Creation Services: Hosting Unit Service Snapin The snap-in that provides information about the hypervisors. AD Identity Service Snapin The snap-in that provides information about the identity pools.

The provisioning scheme is a collection of all of the data that is required to form a template against which virtual machines can be created. It therefore requires the following: Hosting Unit A reference to an item defined in the Host Service that defines the hypervisor, the network, and the storage to be used. Identity Pool A reference to the collection of Active Directory accounts that is used for virtual machines created from the provisioning scheme.

Related topics

Get-ProvTask

Get-ProvScheme

Test-ProvSchemeNameAvailable

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme to be created. This must be a name that is not being used by an existing provisioning scheme, and it must not contain any of the following characters \/:;#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-HostingUnitName<String>

The name of the hosting unit used for the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IdentityPoolName<String>

The name for the identity pool used for the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	false

-HostingUnitUid<Guid>

The identifier for the hosting unit used for the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IdentityPoolUid<Guid>

The identifier of the identity pool used for the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MasterImageVM<String>

The path in the hosting unit provider to the virtual machine snapshot that is used. This identifies the hard disk to be used and the default values for the memory and processors. This must be a path to a Snapshot item in the same hosting unit that the hosting unit name or hosting unit UID refers to.

Valid paths are of the format; XDHyp:\HostingUnits\<HostingUnitName>\<path>\<VmName>.vm\<SnapshotName>.snapshot

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-VMCpuCount<Int32>

The number of processors used by virtual machines created from the provisioning scheme.

Required?	false
Default Value	The number of CPUs assigned to the base image VM snapshot.
Accept Pipeline Input?	false

-VMMemoryMB<Int32>

The maximum amount of memory used by virtual machines created from the provisioning scheme.

Required?	false
Default Value	The amount of memory assigned to the base image VM snapshot.
Accept Pipeline Input?	false

-CleanOnBoot<SwitchParameter>

Indicates whether or not the virtual machines created from this provisioning scheme are reset to their initial condition each time they are started.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-UsePersonalVDiskStorage<SwitchParameter>

Indicates whether or not personal vDisks are used for the VMs in this provisioning scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Scope<String[]>

The administration scopes to be applied to the new provisioning scheme.

Required?	false
Default Value	
Accept Pipeline Input?	false

-NoImagePreparation<SwitchParameter>

Indicates that Image Preparation should not be performed on this Provisioning Scheme

Required?	false
Default Value	
Accept Pipeline Input?	false

-NetworkMapping<Hashtable>

Specifies how the attached NICs are mapped to networks. If this parameter is omitted, provisioned VMs are created with a single NIC, which is mapped to the default network in the HostingUnit. If this parameter is supplied, machines are created with the number of NICs specified in the map, and each NIC is attached to the specified network.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Metadata<Hashtable>

Specifies any metadata to be attached to the scheme when it is created.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceOffering<String>

The Service Offering to use when creating machines in Cloud Hypervisors.

Required?	false
Default Value	
Accept Pipeline Input?	false

-SecurityGroup<String[]>

The security groups to apply to machines created in Cloud Hypervisors

Required?	false
Default Value	
Accept Pipeline Input?	false

-DedicatedTenancy<SwitchParameter>

Whether to use dedicated tenancy when creating machines in Cloud Hypervisors.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-VhdTemplateSource<String>

A file path to a source VHD template to be used when performing Application Scanning during Image Preparation. The presence of this parameter in conjunction with VhdResultDestination implies that application scanning is to be performed

Required?	false
Default Value	
Accept Pipeline Input?	false

-VhdResultDestination<String>

A file path (including file name) where the VHD disk file containing the results of application scanning should be written.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AppScanResultsFile<String>

File name to which the results of application scanning should be written.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ResetAdministratorPasswords<SwitchParameter>

Indicates whether to reset the password for the administrator accounts on provisioned machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RunAsynchronously<SwitchParameter>

Indicates whether or not the command returns before it is complete. If specified, the command returns an identifier for the task that was created. This task can be monitored using the get-ProvTask command.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-PurgeJobOnSuccess<SwitchParameter>

Indicates that the task history is removed from the database when the task has finished. This can only be specified for tasks that are not run asynchronously.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Guid

When the RunAsynchronously identifier is specified, this GUID is returned and provides the task identifier.

System.Management.Automation.PSCustomObject

This object provides details of the task that was run and contains the following information:

TaskId <Guid>

The identifier for the task that was performed.

Active <Boolean>

Indicates whether the task is still processing or is complete.

Host <string>

The name of the host on which the task is running or was run.

DateStarted <DateTime>

The date and time that the task was initiated.

Type <Citrix.XDInterServiceTypes.JobType>

The type of task. For new provisioning scheme tasks, this is always NewProvisioningScheme.

Metadata <Citrix.MachineCreation.Sdk.Metadata[]>

The list of metadata stored against the task. For new tasks, this is empty until metadata is added.

WorkflowStatus <System.Workflow.Runtime.WorkflowStatus>

Indicates the status of the workflow that is used to process the task.

ProvisioningSchemeName <string>

The name of the provisioning scheme that the task was for.

ProvisioningSchemeUid <Guid>

The unique identifier of the provisioning scheme that the task was for.

MasterImage <string>

The path (in the hosting unit provider) of the virtual machine snapshot that was used as the master VM image for the task.

IdentityPoolName <string>

The name of the identity pool (from the ADIdentity PowerShell snap-in) that the new provisioning scheme uses.

IdentityPoolUid <guid>

The unique identifier name of the identity pool (from the ADIdentity PowerShell snap-in) that the new provisioning scheme uses.

HostingUnitName <string>

The name of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme uses.

HostingUnitUid

The unique identifier of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme uses.

PersonalVDiskDriveLetter

The drive letter on which a personal vDisk is mounted (blank if the personal vDisk feature was not selected).

PersonalVDiskDriveSize

The size of any personal vDisk (zero if the personal vDisk feature was not selected).

Scopes <Citrix.Fma.Sdk.ServiceCoreScopeReference[]>

The delegated administration scopes to which the scheme will belong.

NetworkMap <Citrix.MachineCreation.Sdk.NetworkMap>

The list of NIC to network associations, if specified.

ProvisioningSchemeMetadata <Dictionary<string, string>>

The metadata to apply to the provisioning scheme, if specified.

TaskState <Citrix.MachineCreation.Sdk.NewProvisioningSchemeState>

The state of the task. This can be any of the following:

Processing

The task has begun but has not done anything yet.

LocatingResources,

The workflow is locating resources from other services.

HostingUnitNotFound

The task failed because the required hosting unit could not be located.

VirtualMachineSnapshotNotFound

The task failed because the required VM snapshot could not be located.

ConsolidatingMasterImage

The task is consolidating the master image.

ReplicatingConsolidatedImageToAllStorage

The task is replicating the consolidated master image.

StoringProvisioningScheme

The task is storing the provisioning scheme data in the database.

Finished

The task completed with no errors.

ProvisioningSchemeAlreadyExists

The task failed because a provisioning scheme with the same name already exists.

IdentityPoolNotFound

The task failed because the specified identity pool could not be found.

MasterVMImageIsNotPartOfProvisioningSchemeHostingUnit,

The task failed because the hosting unit from which the master image originated is not the same hosting unit that the provisioning scheme is using.

MasterVmImageIsASnapshot

The task failed because the master VM path does not refer to a Snapshot item.

ProvisioningSchemeNotFound

The task failed because it could not find a provisioning scheme with the specified name.

TaskAlreadyRunningForProvisioningScheme

The task failed because a task for a provisioning scheme with the same name is already running.

InvalidMasterVMConfiguration

The task failed because the VM snapshot specified as the master has an invalid configuration.

InvalidMasterVMState

The task failed because the VM snapshot specified as the master is currently in an invalid state.

InsufficientResources

The task failed because the hypervisor did not have enough resources to complete the task.

DiskConsolidationFailed

The disk consolidation task failed. Details are in the task state information string.

StorageNotFound

The task failed because no associated storage was found in the hosting unit.

ConfigurationError

The task failed because the service is unable to contact one of the other services. This is because not all appropriate Configuration Service registrations have been performed.

Canceled

The task was stopped by user intervention (using Stop-ProvTask).

TaskStateInformation

Additional information about the current task state.

TaskProgress

The progress of the task 0-100%.

DiskSize

The size of the master image in GB

DedicatedTenancy

Whether to use dedicated tenancy when creating machines in Cloud Hypervisors.

Notes

Only one long-running task for each provisioning scheme can be processed at a time.

In case of failure, the following errors can result.

Error Codes

JobCreationFailed

The requested task could not be started.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation. Communication with the database failed for

for various reasons.

MachineCreationServiceDoesNotSupportPersonalDisk

The service instance being used has not been upgraded to support the personal vDisk feature.

DatabaseMissingCapabilites

The database supporting the service instance being used has not been upgraded to support the personal vDisk feature.

CommunicationError

An error occurred while communicating with the service.

InvalidParameterCombination

Both PurgeJobOnSuccess and RunAsynchronously were specified. When running asynchronously, the cmdlet terminates before the job does, so it cannot clean up the completed job.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

ScopeNotFound

One or more of the scopes nominated for the new provisioning scheme do not exist.

WorkflowHostUnavailable

The task could not be started because the database connection is inactive.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used, or examine the XenDesktop logs. VhdParametersMustBeSupplied

When parameter VhdTemplateSource or VhdResultDestination is supplied, both parameters are required to be supplied.

The cmdlet is associated with a task of type NewProvisioningScheme, and while active will move through the following operations (CurrentOperation field)

ValidatingInputs

ConsolidatingMasterImage

PreparingMasterImage

ReplicatingMasterImage

CommittingScheme

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName XenHu -IdentityPoo
lName idPool1 -CleanOnBoot -MasterImageVM XDHyp:\HostingUnits\XenHU\Base.vm\Base.snapshot

TaskId                      : 90e93b9d-a225-4701-ad50-fa1546af35ac
Active                      : False
Host                        : MyHost
DateStarted                 : 17/05/2010 08:22:22
Type                        : NewProvisioningScheme
Metadata                    : {}
WorkflowStatus              : Completed
ProvisioningSchemeName      : XenPS
MasterImage                 : /Base.vm/Base.snapshot
IdentityPoolName            : idPool1
IdentityPoolUid             : 03743136-e43b-4a87-af74-ab71686b3c16
HostingUnitName             : XenHU
HostingUnitUid              : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
PersonalVDiskDriveLetter    :
PersonalVDiskDriveSize      : 0
ProvisioningSchemeUid       : 7585f0de-192e-4847-a6d8-22713c3a2f42
CurrentOperation            :
TaskState                   : Finished
TaskStateInformation        :
TaskProgress                : 100
DiskSize                    : 24
```

Creates a new provisioning scheme with the name "XenPS" using the hosting unit "XenHu" and the identity pool "idPool1" from the master VM snapshot called "Base.snapshot".

---------- EXAMPLE 2 ----------

```
C:\PS> New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName XenHu -IdentityPoolName idPool1 -CleanOnBoot -MasterImageVM XDHyp:\HostingUnits\XenHU

Guid
----
6dd85fec-96cf-46b1-9cd4-d8ba7d06e85b
```

Creates a new provisioning scheme with the name "XenPS" using the hosting unit "XenHu" and the identity pool "idPool1" from the master VM snapshot called "Base.snapshot" asynchronously. To get the task details, use Get-ProvTask -TaskID <task id>

i.e.

C:\PS>Get-ProvTask -TaskID 6dd85fec-96cf-46b1-9cd4-d8ba7d06e85b

TaskId : 6dd85fec-96cf-46b1-9cd4-d8ba7d06e85b

Active : False

Host : MyHost

DateStarted : 17/05/2010 08:22:22

Type : NewProvisioningScheme

Metadata : {}

WorkflowStatus : Completed

ProvisioningSchemeName : XenPS

MasterImage : XDHyp:\HostingUnits\XenHU\Base.vm\Base.snapshot

IdentityPoolName : idPool1

IdentityPoolUid : 03743136-e43b-4a87-af74-ab71686b3c16

HostingUnitName : XenHU

HostingUnitUid : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501

PersonalVDiskDriveLetter :

PersonalVDiskDriveSize : 0

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

TaskState : Finished

TaskStateInformation :

TaskProgress : 100

DiskSize : 24

---------- EXAMPLE 3 ----------

C:\PS>$provScheme = New-ProvScheme -ProvisioningSchemeName XenPS2 -HostingUnitName XenHu -IdentityPoolName idPool1 -CleanOnBoot -MasterImageVM XDHyp:\Ho
Creates a new provisioning scheme with the name "XenPS2" using the hosting unit "XenHu" and the identity pool "idPool1" from the master VM snapshot called "Base.snapshot"; apply a 17GB personal vDisk. The personal vDisk is mapped as drive X. The operation runs synchronously, and the return value contains the task details

For example:

C:\PS>$provScheme

TaskId : d726222a-04b5-4098-b9ac-db85ed9d351b

Active : False

Host : MyHost

DateStarted : 12/09/2011 09:30:04

Type : NewProvisioningScheme

Metadata : {}

ProvisioningSchemeName : XenPS2

IdentityPoolName : idPool1

IdentityPoolUid : 03743136-e43b-4a87-af74-ab71686b3c16

HostingUnitName : XenHU

HostingUnitUid : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501

PersonalVDiskDriveLetter : X

PersonalVDiskDriveSize : 17

WorkflowStatus : Completed

MasterImage : XDHyp:\HostingUnits\XenHU\Base.vm\Base.snapshot

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

TaskState : Finished

TaskStateInformation :

TaskProgress : 100

DiskSize : 24

New-ProvVM

Sep 10, 2014

Creates a new virtual machine.

Syntax

New-ProvVM -ProvisioningSchemeName <String> -ADAccountName <String[]> [-FastBuild] [-NetworkMapping <Hashtable>] [-AutoAssignVLAN] [-SecurityGroup <String[]>] [-MachinesPerAssistant <Int32>] [-MaxAssistants <Int32>] [-RunAsynchronously] [-PurgeJobOnSuccess] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

New-ProvVM -ProvisioningSchemeUid <Guid> -ADAccountName <String[]> [-FastBuild] [-NetworkMapping <Hashtable>] [-AutoAssignVLAN] [-SecurityGroup <String[]>] [-MachinesPerAssistant <Int32>] [-MaxAssistants <Int32>] [-RunAsynchronously] [-PurgeJobOnSuccess] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Lets you create new virtual machines with the configuration specified by a provisioning scheme.

The virtual machines are created using all of the storage specified in the provisioning scheme. The storage is used in a round robin mechanism. For the duration of this task, the AD accounts are locked (by the AD Identity Service), which stops the same accounts being used by other virtual machine creation tasks.

Related topics

Get-ProvVM

Remove-ProvVM

Lock-ProvVM

Unlock-ProvVM

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme in which the virtual machines are created.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ProvisioningSchemeUid<Guid>

The unique identifier for the provisioning scheme in which the virtual machines are created.

Required?	true

Default Value	
Accept Pipeline Input?	false

-ADAccountName<String[]>

A list of the Active Directory account names that are used for the virtual machines. The accounts must be provided in a domain-qualified format. This parameter accepts Identity objects as returned by the New-AcctADAccount cmdlet, or any PSObject with string properties "Domain" and "ADAccountName".

Required?	true
Default Value	
Accept Pipeline Input?	false

-FastBuild<SwitchParameter>

Indicates whether or not the command can improve speed by using optimizations in the creation process. This may mean that machines you create cannot be booted until ResetVM operations have been performed by the Broker and Machine Identity Services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-NetworkMapping<Hashtable>

Specifies how the attached NICs are mapped to networks. If this parameter is omitted, provisioned VMs are created with network settings as inherited from the provisioning scheme. If this parameter is supplied, machines are created with the number of NICs specified in the map, and each NIC is attached to the specified network.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AutoAssignVLAN<SwitchParameter>

Indicates whether or not the VLAN of the network should be automatically assigned to the new VM or if the VLAN from the master image should be used

Required?	false

Default Value	false
Accept Pipeline Input?	false

-SecurityGroup<String[]>

The security groups to apply to machines created in Cloud Hypervisors

Required?	false
Default Value	
Accept Pipeline Input?	false

-MachinesPerAssistant<Int32>

The number of concurrent volume operations that may be performed by each volume worker helper machine

Required?	false
Default Value	
Accept Pipeline Input?	false

-MaxAssistants<Int32>

The maximum number of volume worker help machines that may be created for this operation.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RunAsynchronously<SwitchParameter>

Indicates whether or not the command returns before it is complete. If specified, the command returns an identifier for the task that was created. This task can be monitored using the get-ProvTask command.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-PurgeJobOnSuccess<SwitchParameter>

Indicates that the task history is removed from the database when the task has finished. This cannot be specified for tasks that are run asynchronously.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller to which the PowerShell snap-in connects. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Guid

When the RunAsynchronously identifier is specified, this GUID is returned and provides the task identifier.

System.Management.Automation.PSCustomObject

This object provides details of the task that was run and contains the following information:

TaskId <Guid>

The identifier for the task that was performed.

Active <Boolean>

Indicates whether the task is still processing or is complete.

Host <string>

The name of the host on which the task is running or was run.

DateStarted <DateTime>

The date and time that the task was initiated.

Type <Citrix.XDInterServiceTypes.JobType>

The type of task. For newly provisioned VM tasks, this is always "NewVirtualMachine".

Metadata <Citrix.MachineCreation.Sdk.Metadata[]>

The list of metadata stored against the task. For new tasks this is empty until metadata is added.

WorkflowStatus <System.Workflow.Runtime.WorkflowStatus>

Indicates the status of the workflow that is used to process the task.

ProvisioningSchemeName <string>

The name of the provisioning scheme that the task was for.

ProvisioningSchemeUid <Guid>

The unique identifier of the provisioning scheme that the task was for.

MasterImage <string>

The path (in the hosting unit provider) of the virtual machine snapshot that was used as the master image for the task.

IdentityPoolName <string>

The name of the identity pool (from the ADIdentity PowerShell snap-in) that the new provisioning scheme uses.

IdentityPoolUid <guid>

The unique identifier name of the identity pool (from the ADIdentity PowerShell snap-in) that the new provisioning scheme uses.

HostingUnitName <string>

The name of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme uses.

HostingUnitUid

The unique identifier of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme uses.

TaskState <Citrix.DesktopUpdateManager.SDK.ProvisionVMState>

The state of the task. This can be any of the following:

Processing

Indicates that the task is in its initial state.

LocatingResources,

Indicates that the task is locating information from other services.

HostingUnitNotFound

Indicates that the required hosting unit could not be located.

ProvisioningSchemeNotFound

Indicates that the required provisioning scheme could not be located.

Provisioning

Indicates that the task is at the provisioning stage.

IdentityPoolNotFound

Indicates that the required identity pool could not be located.

TaskAlreadyRunningForProvisioningScheme

Indicates that the provisioning scheme already has another task running.

HypervisorInMaintenanceMode

Indicates that the hypervisor is not available for normal use.

NoAvailableStorage

Indicates that no storage is available for the hypervisor.

NoAvailableNetwork

Indicates that no network is available for the hypervisor.

Finalizing

Indicates that the task is finalizing.

Finished

Indicates that the task is complete.

FinishedWithErrors

Indicates that the task is complete but there were errors. Specific details of errors are included with each failed virtual machine.

Removing

Indicates that the task is removing virtual machines from the hypervisor.

Failed

The job failed for reasons specified in TaskStateInformation.

Canceled

Indicates that the task was stopped by user intervention (using Stop-ProvTask).

TaskStateInformation

Provides more detailed information about the current task state.

VirtualMachinesToCreateCount <int>

The total number of virtual machines that the task is trying to create.

VirtualMachinesCreatedCount <int>

The number of virtual machines that the task has created so far. Details of the machines that were created are in the CreatedVirtualMachines parameter.

VirtualMachinesCreationFailedCount <int>

The number of virtual machines that the task has failed to create. Details of the machines that were not created are in the FailedVirtualMachines parameter.

FailedVirtualMachines <Citrix.DesktopUpdateManager.SDK.VirtualMachineCreation[]>

ADAccountName <string>

The domain qualified AD Account name of the machine.

ADAccountSid <string>

The AD account SID of the machine account.

DiagnosticInformation <Citrix.MachineCreation.Sdk.ExceptionSurrogate[]>

A collection of handled error states which caused the provisioning to fail.

ExceptionType <string>

The type of exception this object represents

Message <string>

The exception message

Details <string>

The full exception content including stack trace

InnerException <Citrix.MachineCreation.Sdk.ExceptionSurrogate>

Information relating to any contributing error state

Status <string>

StatusAdditionalInformation <string>

VMId <string>

The virtual machine identifier within the hypervisor in which the VM resides.

VMName <string>

The display name of the virtual machine within the hypervisor in which the VM resides.

CreatedVirtualMachines <Citrix.DesktopUpdateManager.SDK.VirtualMachineCreation[]>

See FailedVirtualMachines for details of the object parameters.

Notes

Only one long-running task in each provisioning scheme can be processed at a time.

In the case of failure, the following errors can result.

Error Codes

JobCreationFailed

The requested task could not be started.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation. Communication with the database failed

for various reasons.

WorkflowHostUnavailable

The task could not be started because the database connection is inactive.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

CommunicationError

An error occurred while communicating with the service.

InvalidParameterCombination

Both PurgeJobOnSuccess and RunAsynchronously were specified.

When running asynchronously, the cmdlet terminates before the job does,

so it cannot clean up the completed job.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs

on the controller being used, or examine the XenDesktop logs.

The cmdlet is associated with a task of type NewVirtualMachine, and while active will move through the following operations (CurrentOperation field)

ValidatingInputs

CreatingVirtualMachines

ReleasingAccountLocks

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>New-provVM -ProvisioningSchemeName MyScheme -ADAccountName "domain\Account"

TaskId                        : 4b49f13a-277c-4cb0-bc40-f088430cfe8a
Active                        : False
Host                          : DUMTESTDDC
DateStarted                   : 18/05/2010 10:54:32
Type                          : NewVirtualMachine
Metadata                      : {}
WorkflowStatus                : Completed
MasterImage                   : /Base.vm/Base.snapshot
ProvisioningSchemeName        : MyScheme
ProvisioningSchemeUid         : 7585f0de-192e-4847-a6d8-22713c3a2f42
CurrentOperation              :
TaskState                     : Finished
TaskStateInformation          :
HostingUnitUid                : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
HostingUnitName               : XenHU
IdentityPoolUid               : 03743136-e43b-4a87-af74-ab71686b3c16
IdentityPoolName              : idPool1
VirtualMachinesToCreateCount  : 1
VirtualMachinesCreatedCount   : 1
VirtualMachinesCreationFailedCount : 0
CreatedVirtualMachines        : {DOMAIN\Account$}
FailedVirtualMachines         : {}
ProvisioningJob               : 6fa5dc7c-6d49-4616-8682-aeb1580866b3
ProvisioningStatus            : Completed
```

Creates a new virtual machine using the AD account "domain\account" in the provisioning scheme "MyScheme".

---------- EXAMPLE 2 ----------

```
C:\PS>New-provVM -ProvisioningSchemeName MyScheme -ADAccountName "domain\Account" -RunAsynchronously

Guid
----
6dd85fec-96cf-46b1-9cd4-d8ba7d06e85b
```

Creates a new virtual machine using the AD account "domain\account" in the provisioning scheme "MyScheme" asynchronously. To get the task details, use Get-ProvTask -TaskID <task id>

i.e.

```
C:\PS>Get-ProvTask -TaskID 6dd85fec-96cf-46b1-9cd4-d8ba7d06e85b
```

TaskId : 4b49f13a-277c-4cb0-bc40-f088430cfe8a

Active : False

Host : MyHost

DateStarted : 18/05/2010 10:54:32

Type : NewVirtualMachine

Metadata : {}

WorkflowStatus : Completed

MasterImage : /Base.vm/Base.snapshot

ProvisioningSchemeName : MyScheme

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

TaskState : Finished

TaskStateInformation :

HostingUnitUid : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501

HostingUnitName : XenHU

IdentityPoolUid : 03743136-e43b-4a87-af74-ab71686b3c16

IdentityPoolName : idPool1

VirtualMachinesToCreateCount : 1

VirtualMachinesCreatedCount : 1

VirtualMachinesCreationFailedCount : 0

CreatedVirtualMachines : {DOMAIN\Account$}

FailedVirtualMachines : {}

ProvisioningJob : 6fa5dc7c-6d49-4616-8682-aeb1580866b3

ProvisioningStatus : Completed

---------- **EXAMPLE 3** ----------

C:\PS>$accounts = Get-AcctAdAccount -IdentityPool MyPool -State Available
C:\PS>New-provVM -ProvisioningSchemeName MyScheme -ADAccountName $t -RunAsyncronously
Creates a new virtual machine using all of the available AD accounts from the identity pool "MyPool" in the provisioning scheme "MyScheme" asynchronously. To get the task details, use Get-ProvTask -TaskID <task id>

For example:

C:\PS>Get-ProvTask -TaskID 6dd85fec-96cf-46b1-9cd4-d8ba7d06e85b

TaskId : 4b49f13a-277c-4cb0-bc40-f088430cfe8a

Active : False

Host : MyHost

DateStarted : 18/05/2010 10:54:32

Type : NewVirtualMachine

Metadata : {}

WorkflowStatus : Completed

MasterImage : /Base.vm/Base.snapshot

ProvisioningSchemeName : MyScheme

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

TaskState : Finished

TaskStateInformation :

HostingUnitUid : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501

HostingUnitName : XenHU

IdentityPoolUid : 03743136-e43b-4a87-af74-ab71686b3c16

IdentityPoolName : idPool1

VirtualMachinesToCreateCount : 1

VirtualMachinesCreatedCount : 1

VirtualMachinesCreationFailedCount : 0

CreatedVirtualMachines : {DOMAIN\Account$}

FailedVirtualMachines : {}

ProvisioningJob : 6fa5dc7c-6d49-4616-8682-aeb1580866b3

ProvisioningStatus : Completed

Publish-ProvMasterVmImage

Sep 10, 2014

Update the master image associated with the provisioning scheme.

Syntax

```
Publish-ProvMasterVmImage [-ProvisioningSchemeName] <String> -MasterImageVM <String> [-DoNotStoreOldImage] [-VhdTemplateSource <String>] [-VhdResultDestination <String>] [-AppScanResultsFile <String>] [-RunAsynchronously] [-PurgeJobOnSuccess] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Publish-ProvMasterVmImage -ProvisioningSchemeUid <Guid> -MasterImageVM <String> [-DoNotStoreOldImage] [-VhdTemplateSource <String>] [-VhdResultDestination <String>] [-AppScanResultsFile <String>] [-RunAsynchronously] [-PurgeJobOnSuccess] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to update the hard disk image used to provision virtual machines. If the provisioning scheme is a 'CleanOnBoot' type, then the next time that virtual machines are started, their hard disks are updated to this new image. Regardless of the 'CleanOnBoot' type, all new virtual machines created after this command will use this new hard disk image.

A background task will be created to remove the old hard disk copies. You can locate and monitor this task using the Get-ProvTask cmdlet.

A snapshot is used rather than a VM, so that the content of the hard disk for the provisioning scheme can be easily determined.

As the snapshot is specified using a path into the Citrix Host Service Powershell Provider, the Citrix Host Service Powershell snap-in must also be loaded for this cmdlet to be used.

The previous hard disk image path is stored into the history (see Get-provSchemeMasterVMImageHistory). The data stored in the history allows for a roll back to be undertaken, to revert to the previous hard disk image if required.

Related topics

Get-ProvSchemeMasterVMImageHistory

Get-ProvScheme

Parameters

-ProvisioningSchemeName<String>

The provisioning scheme to which the hard disk image should be updated.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeUid<Guid>

The provisioning scheme identifier to which the hard disk image should be updated.

Required?	true
Default Value	
Accept Pipeline Input?	false

-MasterImageVM<String>

The path in the hosting unit provider to the virtual machine snapshot that will be used. This identifies the hard disk to be used and the default values for the memory and processors. This must be a path to a Snapshot Item in the same hosting unit that the hosting unit name or hosting unit Uid refers to.

Valid paths are of the format; XDHyp:\HostingUnits\<HostingUnitName>\<path>\<VmName>.vm\<SnapshotName>.snapshot

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-DoNotStoreOldImage<SwitchParameter>

Specifies that the current image should not be added to the image history list for the provisioning scheme. This is useful when rolling back to a previous image.

Required?	false
Default Value	
Accept Pipeline Input?	false

-VhdTemplateSource<String>

A file path to a source VHD template to be used when performing Application Scanning during Image Preparation. The

presence of this parameter in conjunction with VhdResultDestination implies that application scanning is to be performed

Required?	false
Default Value	
Accept Pipeline Input?	false

-VhdResultDestination<String>

A file path (including file name) where the VHD disk file containing the results of application scanning should be written.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AppScanResultsFile<String>

File name to which the results of application scanning should be written.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RunAsynchronously<SwitchParameter>

Indicates whether or not the cmdlet should return before it is complete. If specified, the command returns an identifier for the task that was created. You can monitor this task using the get-ProvTask cmdlet.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-PurgeJobOnSuccess<SwitchParameter>

Indicates that the task history will be removed from the database once the task has finished. This cannot be specified for

tasks that are run asynchronously.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Guid

When "RunAsynchronously" is specified, this identifier is returned to provide the task identifier.

System.Management.Automation.PSCustomObject

This object provides details of the task run and contains the following information:

TaskId <Guid>

The identifier for the task that was performed.

Active <Boolean>

Indicates whether the task is still processing or is complete.

Host <string>

The name of the host on which the task is running or was run.

DateStarted <DateTime>

The date and time that the task was initiated.

Type <Citrix.XDInterServiceTypes.JobType>

The type of the task. For new provisioning scheme tasks this is always "NewProvisioningScheme".

Metadata <Citrix.MachineCreation.Sdk.Metadata[]>

The list of metadata stored against the task. For new tasks this will be empty until metadata is added.

WorkflowStatus <System.Workflow.Runtime.WorkflowStatus>

Indicates the status of the workflow that is being used to process the task.

ProvisioningSchemeName <string>

The name of the provisioning scheme that the task was for.

ProvisioningSchemeUid <Guid>

The unique identifier of the provisioning scheme that the task was for.

MasterImage <string>

The path (in the hosting unit provider) of the virtual machine snapshot that was used as the master image for the task.

IdentityPoolName <string>

The name of the identity pool (from the ADIdentity PowerShell snap-in) that the new provisioning scheme will use.

IdentityPoolUid <guid>

The unique identifier name of the identity pool (from the ADIdentity PowerShell snap-in) that the new provisioning scheme will use.

HostingUnitName <string>

The name of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme will use.

HostingUnitUid

The unique identifier of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme will use.

TaskState <Citrix.DesktopUpdateManager.SDK.NewProvisioningSchemeState>

The state of the task. This can be any of the following:

Processing

Indicates that the task has just begun and has not done anything yet.

LocatingResources,

Indicates that the workflow is locating resources from other services.

HostingUnitNotFound

Indicates that the task failed because the required hosting unit could not be located.

VirtualMachineSnapshotNotFound

Indicates that the task failed because the required snapshot could not be located.

ConsolidatingMasterImage

Indicates that the task is consolidating the master image.

ReplicatingConsolidatedImageToAllStorage

Indicates that the task is replicating the consolidated master image.

StoringProvisioningScheme

Indicates that the task is storing the provisioning scheme data to the database.

Finished

Indicates that the task has completed with no errors.

ProvisioningSchemeAlreadyExists

Indicates that the task failed because a provisioning scheme with the same name already exists.

IdentityPoolNotFound

Indicates that the task failed because the identity pool specified could not be found.

MasterVMImageIsNotPartOfProvisioningSchemeHostingUnit,

Indicates that the hosting unit that the master image originated from is not the same hosting unit that the provisioning scheme is defined to use.

MasterVmImageIsNotASnapshot

Indicates that the task failed because the master VM Image path does not refer to a Snapshot item.

ProvisioningSchemeNotFound

Could not find a provisioning scheme with the specified name.

TaskAlreadyRunningForProvisioningScheme

A task for a provisioning scheme with the same name is already running.

InvalidMasterVMConfiguration

The VM snapshot specified as the master had an invalid configuration.

InvalidMasterVMState

The VM snapshot specified as the master is currently in an invalid state.

InsufficientResources

Indicates that the task failed because the hypervisor did not have enough resources to complete the task.

StorageNotFound

Indicates that no associated storage was found in the hosting unit.

Canceled

Indicates that the task was stopped by user intervention (using Stop-ProvTask)

TaskStateInformation <string>

Holds string data providing more details about the current task state.

TaskProgress

The progress of the task 0-100%.

Notes

Only one long running task per provisioning scheme can be processed at any one time.

In the case of failure, the following errors can result.

Error Codes

JobCreationFailed

The requested task could not be started.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

WorkflowHostUnavailable

The task could not be started because the database connection is inactive.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

The cmdlet is associated with a task of type PublishImage, and while active will move through the following operations (CurrentOperation field)

ValidatingInputs

ConsolidatingMasterImage

PreparingMasterImage

ReplicatingMasterImage

CommittingScheme

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -MasterImageVM XDHyp:\H
stingUnits\HostUnit1\RhoneCC_baseXP.vm\base.snapshot

TaskId              : 248f102f-073f-45fe-aea9-1819a6d6dd1f
Active              : False
Host                : MyHost
DateStarted         : 17/05/2010 17:37:57
Type                : PublishImage
Metadata            : {}
WorkflowStatus      : Completed
ProvisioningSchemeUid  : 7585f0de-192e-4847-a6d8-22713c3a2f42
ProvisioningSchemeName : MyScheme
MasterImage         : /RhoneCC_baseXP.vm/base.snapshot
HostingUnitName     : HostUnit1
```



```
HostingUnitUid       : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
ADIdentityPoolName   :
ADIdentityPoolUid    : 03743136-e43b-4a87-af74-ab71686b3c16
CurrentOperation     :
TaskState            : Finished
TaskStateInformation :
```

Updates the master hard disk image for the provisioning Scheme "MyScheme" to use the "base.snapshot" hard disk image.

Remove-ProvScheme

Sep 10, 2014

Removes a provisioning scheme

Syntax

```
Remove-ProvScheme [-ProvisioningSchemeName] <String> [-ForgetVM] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvScheme -ProvisioningSchemeUid <Guid> [-ForgetVM] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove a provisioning Scheme. The provisioning scheme must not contain any VMs unless the 'ForgetVM' option is specified.

If 'ForgetVM' is not specified, a cmdlet task is created that runs in the background to remove the hard disk copies that have been created for the provisioning scheme in hypervisor storage. Use the Get-ProvTask command to monitor the progress of this task.

Related topics

Get-ProvTask

New-ProvScheme

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeUid<Guid>

The unique identifier for the provisioning scheme to be removed.

Required?	true
Default Value	

Accept Pipeline Input?	true (ByPropertyName)

-ForgetVM<SwitchParameter>

Indicates whether or not the VMs in the provisioning scheme should be left in the hypervisor and only the data held in the Machine Creation Services removed. If this is specified, it is up to the administrator of the hypervisor to remove the VMs and hard disk images using the tools provided by the hypervisor itself.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.ProvisioningScheme

This object provides details of the provisioning scheme and contains the following information:

ProvisioningSchemeUid

The unique identifier for the provisioning scheme.

ProvisioningSchemeName

The name of the provisioning scheme.

CpuCount

The number of processors that VMs will be created with when using this scheme.

MemoryMB

The maximum amount of memory that VMs will be created with when using this scheme.

MasterImageVM

The path within the hosting unit provider to the VM or snapshot of which the scheme is currently using a copy.

MasterImageVMDate

The date and time that the copy of the VM image was made for the scheme.

IdentityPoolUid

The unique identifier of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

IdentityPoolName

The name of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

HostingUnitUid

The unique identifier of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme will use.

HostingUnitName

The name of the hosting unit (from the hosting unit PowerShell snap-in) that the new provisioning scheme will use.

CleanOnBoot

Indicates whether the VMs created are to be reset to a clean state on each boot.

TaskId

The identifier of any current task that is running for the provisioning scheme.

Notes

If the hosting unit referenced by the provisioning scheme no longer exists (i.e. it has been removed using the Hosting Unit PowerShell snap-in), the provisioning scheme data is deleted from the database without errors. However, the hard disks associated with the provisioning scheme cannot be removed and remain in the hypervisor.

In the case of failure, the following errors can result.

Error Codes

IllegalParameter

One or more parameters are illegal or are not specified.

ProvisioningSchemeNotFound

The specified provisioning scheme could not be located.

UnableToRemoveProvisioningSchemeDueToAssociatedVM

The provisioning scheme contained VMs and the 'ForgetVM' parameter was not specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

The cmdlet is associated with a task of type DisusedImageCleanUp, and while active will move through the following operations (CurrentOperation field)

Running

Examples

---------- EXAMPLE 1 ----------


```
c:\PS>Remove-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
```

Remove the empty provisioning scheme by name.

Remove-ProvSchemeControllerAddress

Sep 10, 2014

Removes metadata from a provisioning scheme.

Syntax

```
Remove-ProvSchemeControllerAddress [-ProvisioningSchemeName] <String> [-ControllerAddress] <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeControllerAddress -ProvisioningSchemeUid <Guid> -ControllerAddress <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Removes the specified controller addresses from the specified object. Attempting to remove an address not present writes an error record to the pipeline.

Related topics

Get-ProvScheme

Add-ProvSchemeControllerAddress

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme from which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeUid<Guid>

The identifier of the provisioning scheme from which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ControllerAddress<String[]>

Specifies the array of DNS names to be removed from the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.MachineCreation.Sdk.ProvisioningScheme You can pipe an object containing a parameter called 'ProvisioningSchemeName' to Remove-ProvSchemeMetadata.

Notes

In the case of failure, the following errors can result.

Error Codes

ProvisioningSchemeNotFound

The specified provisioning scheme could not be located.

ControllerAddressNotFound

The specified address was not associated with the provisioning scheme.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Get-ProvScheme -ProvisioningSchemeName scheme1 | Remove-ProvSchemeControllerAddress

ProvisioningSchemeUid  : 7585f0de-192e-4847-a6d8-22713c3a2f42
ProvisioningSchemeName : Scheme1
CpuCount               : 1
MemoryMB               : 1024
MasterImageVM          : Base.vm/Base.snapshot
MasterImageVMDate      : 17/05/2010 09:53:40
IdentityPoolUid        : 03743136-e43b-4a87-af74-ab71686b3c16
IdentityPoolName       : idPool1
HostingUnitUid         : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
HostingUnitName        : HostUnit1
CleanOnBoot            : True
TaskId                 : 00000000-0000-0000-0000-000000000000
Metadata               : {}
ControllerAddress      : {}
```

Remove all controller addresses from the provisioning scheme with the name "scheme1".

---------- EXAMPLE 2 ----------

```
C:\PS>Remove-ProvSchemeControllerAddress -ProvisioningSchemeUid "01a4a008-8ce8-4165-ba9c-cdf15a6b0501" -ControllerAddress (ddcA.citrix.com,ddcC.citrix2.com)

ProvisioningSchemeUid  : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
ProvisioningSchemeName : Scheme2
CpuCount               : 1
```

```
MemoryMB              : 1024
MasterImageVM         : Base.vm/Base.snapshot
MasterImageVMDate     : 17/05/2010 09:53:40
IdentityPoolUid       : 03743136-e43b-4a87-af74-ab71686b3c16
IdentityPoolName      : idPool1
HostingUnitUid        : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
HostingUnitName       : HostUnit1
CleanOnBoot           : True
TaskId                : 00000000-0000-0000-0000-000000000000
Metadata              : {}
ControllerAddress     : {ddcB.citrix.com}
```

Remove a subset of the controller address list from the provisioning scheme with the identifier "01a4a008-8ce8-4165-ba9c-cdf15a6b0501".

Remove-ProvSchemeMasterVMImageHistory

Sep 10, 2014

Removes the history of provisioning scheme master image VMs.

Syntax

Remove-ProvSchemeMasterVMImageHistory [-ProvisioningSchemeName] <String> [-VMImageHistoryUid <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeMasterVMImageHistory -ProvisioningSchemeUid <Guid> [-VMImageHistoryUid <Guid>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeMasterVMImageHistory -VMImageHistoryUid <Guid> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to remove the record of previously used master VMs or snapshots for provisioning schemes.

Related topics

Get-ProvSchemeMasterVMImageHistory

Publish-ProvMasterVMImage

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeUid<Guid>

The unique identifier of the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	false

-VMImageHistoryUid<Guid>

The unique identifier for the Image History item.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

In the case of failure, the following errors can result.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Remove-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName MyScheme
```

Removes all history for the provisioning scheme called "MyScheme".

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ProvScheme | Remove-ProvSchemeMasterVMImageHistory
```

Removes all history for all provisioning schemes.

Remove-ProvSchemeMetadata

Sep 10, 2014

Removes metadata from the given ProvisioningScheme.

Syntax

Remove-ProvSchemeMetadata [-ProvisioningSchemeUid] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeMetadata [-ProvisioningSchemeUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeMetadata [-ProvisioningSchemeName] <String> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeMetadata [-ProvisioningSchemeName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeMetadata [-InputObject] <ProvisioningScheme[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeMetadata [-InputObject] <ProvisioningScheme[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to remove metadata from the given ProvisioningScheme.

Related topics

Add-ProvSchemeMetadata

Set-ProvSchemeMetadata

Parameters

-ProvisioningSchemeUid<Guid>

Id of the ProvisioningScheme

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ProvisioningSchemeName<String>

Name of the ProvisioningScheme

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<ProvisioningScheme[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create

high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvScheme | Remove-ProvSchemeMetadata
```

Remove all metadata from all ProvisioningScheme objects.

Remove-ProvSchemeScope

Sep 10, 2014

Remove the specified ProvisioningScheme(s) from the given scope(s).

Syntax

```
Remove-ProvSchemeScope [-Scope] <String[]> -InputObject <ProvisioningScheme[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeScope [-Scope] <String[]> -ProvisioningSchemeUid <Guid[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvSchemeScope [-Scope] <String[]> -ProvisioningSchemeName <String[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

The RemoveProvSchemeScope cmdlet is used to remove one or more ProvisioningScheme objects from the given scope(s).

There are multiple parameter sets for this cmdlet, allowing you to identify the ProvisioningScheme objects in different ways:

- ProvisioningScheme objects can be piped in or specified by the InputObject parameter

- The ProvisioningSchemeUid parameter specifies objects by ProvisioningSchemeUid

- The ProvisioningSchemeName parameter specifies objects by ProvisioningSchemeName (supports wildcards)

To remove a ProvisioningScheme from a scope you need permission to change the scopes of the ProvisioningScheme.

If the ProvisioningScheme is not in a specified scope, that scope will be silently ignored.

Related topics

Add-ProvSchemeScope

Get-ProvScopedObject

Parameters

-Scope<String[]>

Specifies the scopes to remove the objects from.

Required?	true
Default Value	
Accept Pipeline Input?	false

-InputObject<ProvisioningScheme[]>

Specifies the ProvisioningScheme objects to be removed.

Required?	true

Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ProvisioningSchemeUid<Guid[]>

Specifies the ProvisioningScheme objects to be removed by ProvisioningSchemeUid.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ProvisioningSchemeName<String[]>

Specifies the ProvisioningScheme objects to be removed by ProvisioningSchemeName.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

None

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

ScopeNotFound

One of the specified scopes was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command with the specified objects or scopes.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Remove-ProvSchemeScope Finance -ProvisioningSchemeUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
```

Removes a single ProvisioningScheme from the 'Finance' scope.

---------- EXAMPLE 2 ----------

```
c:\PS>Remove-ProvSchemeScope Finance,Marketing -ProvisioningSchemeUid 6702C5D0-C073-4080-A0EE-EC74CB537C52
```

Removes a single ProvisioningScheme from multiple scopes.

---------- EXAMPLE 3 ----------

```
c:\PS>Get-ProvScheme | Remove-ProvSchemeScope Finance
```
Removes all visible ProvisioningScheme objects from the 'Finance' scope.

---------- EXAMPLE 4 ----------

```
c:\PS>Remove-ProvSchemeScope Finance -ProvisioningSchemeName A*
```
Removes ProvisioningScheme objects with a name starting with an 'A' from the 'Finance' scope.

Remove-ProvServiceConfigurationData

Sep 10, 2014

Removes configuration data from the service.

Syntax

```
Remove-ProvServiceConfigurationData [[-Name] <String>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove data from the MachineCreation Service configuration data.

Related topics

Set-ProvServiceConfigurationData

Get-ProvServiceConfigurationData

Parameters

-Name<String>

The name of the configuration data item to remove.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name

or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

In the case of failure the following errors can be produced.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown An unexpected error occurred. To locate more details see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Remove-ProvServiceConfigurationData -Name "MyName"
```

Removes the configuration data item with name "MyName".

Remove-ProvServiceMetadata

Sep 10, 2014

Removes metadata from the given Service.

Syntax

```
Remove-ProvServiceMetadata [-ServiceHostId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvServiceMetadata [-InputObject] <Service[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Service.

Related topics

Set-ProvServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvService | % { Remove-ProvServiceMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Service objects.

Remove-ProvTask

Sep 10, 2014

Removes from the database completed tasks for the MachineCreation Service.

Syntax

```
Remove-ProvTask [-TaskId] <Guid> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Enables completed tasks that have run within the MachineCreation Service to be removed from the database.

Related topics

Get-ProvTask

Add-ProvTaskMetadata

Remove-ProvTaskMetadata

Parameters

-TaskId<Guid>

Specifies the identifier for the task to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.Management.Automation.PSObject Objects containing the TaskId parameter can be piped to the Remove-ProvTask command.

Notes

If the command fails, the following errors can result.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

InvalidWorkflow

The specified task could not be found.

InvalidWorkflowState

The task was not in an appropriate state for the requested operation.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvTask -active $false | Remove-ProvTask
Success
```

Remove entries for all completed tasks from the MachineCreation Service.

Remove-ProvTaskMetadata

Sep 10, 2014

Removes metadata from the given Task.

Syntax

Remove-ProvTaskMetadata [-TaskId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvTaskMetadata [-TaskId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvTaskMetadata [-InputObject] <Task[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvTaskMetadata [-InputObject] <Task[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to remove metadata from the given Task.

Related topics

Add-ProvTaskMetadata

Set-ProvTaskMetadata

Get-ProvTask

Remove-ProvTask

Stop-ProvTask

Switch-ProvTask

Parameters

-TaskId<Guid>

Id of the Task

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Task[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvTask | Remove-ProvTaskMetadata
```

Remove all metadata from all Task objects.

Remove-ProvVM

Sep 10, 2014

Removes virtual machines.

Syntax

```
Remove-ProvVM [-ProvisioningSchemeName] <String> -VMName <String[]> [-ForgetVM] [-RunAsynchronously] [-PurgeJobOnSuccess] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-ProvVM [-ProvisioningSchemeUid] <Guid> -VMName <String[]> [-ForgetVM] [-RunAsynchronously] [-PurgeJobOnSuccess] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Lets you remove VMs from the Machine Creation Services and the hypervisor that they run on.

Related topics

Get-ProvVM

New-ProvVM

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme from which virtual machines will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeUid<Guid>

The unique identifier for the provisioning scheme from which the virtual machines are removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-VMName<String[]>

List of VM names that will be removed from the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ForgetVM<SwitchParameter>

The named VMs will only be removed from the provisioning scheme database, but will remain in the hypervisor.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RunAsynchronously<SwitchParameter>

Indicates whether or not the command returns before it is complete. If this is specified, the command returns an identifier for the task that was created. This task can be monitored using the get-ProvTask command.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-PurgeJobOnSuccess<SwitchParameter>

Indicates that the task history is removed from the database when the task finishes. This cannot be specified for tasks that are run asynchronously.

Required?	false
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. When a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Guid

When the RunAsynchronously identifier is specified, this GUID is returned and provides the task identifier.

System.Management.Automation.PSCustomObject

This object provides details of the task that was run and contains the following information:

TaskId <Guid>

The identifier for the task that was performed.

Active <Boolean>

Indicates whether the task is still processing or is complete.

Host <string>

The name of the host on which the task is running or was run.

DateStarted <DateTime>

The date and time that the task was initiated.

Type <Citrix.XDInterServiceTypes.JobType>

The type of task. For new remove-VM tasks, this is always "RemoveVirtualMachine".

Metadata <Citrix.MachineCreation.Sdk.Metadata[]>

The list of metadata stored for the task. For new tasks, this is empty until metadata is added.

WorkflowStatus <System.Workflow.Runtime.WorkflowStatus>

Indicates the status of the workflow that is used to process the task.

ProvisioningSchemeName <string>

The name of the provisioning scheme that the task is for.

ProvisioningSchemeUid <Guid>

The unique identifier of the provisioning scheme that the task is for.

TaskState <Citrix.DesktopUpdateManager.SDK.ProvisionVMState>

The state of the task. This can be any of the following:

Processing

Indicates that the task is in its initial state.

LocatingResources,

Indicates that the task is locating information from other services.

HostingUnitNotFound

Indicates that the required hosting unit could not be located.

ProvisioningSchemeNotFound

Indicates that the required provisioning scheme could not be located.

Provisioning

Indicates that the task is at the provisioning stage.

IdentityPoolNotFound

Indicates that the required identity pool could not be located.

TaskAlreadyRunningForProvisioningScheme

Indicates that the provisioning scheme already has another task running.

Finalizing

Indicates that the task is finalizing.

Finished

Indicates that the task is complete.

FinishedWithErrors

Indicates that the task is complete but there were errors. Specific details of errors are included with each failed virtual machine.

Removing

Indicates that the task is removing virtual machines from the hypervisor.

Failed

Job failed for reasons specified in TaskStateInformation.

Canceled

Indicates that the task was stopped by user intervention (using Stop-ProvTask)

TaskStateInformation

Provides more detailed information about the current task state.

VirtualMachinesToRemoveCount <int>

The total number of virtual machines that the task is trying to remove.

VirtualMachinesRemovedCount <int>

The number of virtual machines that the task has removed so far. Details of the machines that have been removed are in the RemovedVirtualMachines parameter.

VirtualMachinesFailedCount <int>

The number of virtual machines that the task has failed to remove. Details of the machines that failed are in the FailedVirtualMachines parameter.

FailedVirtualMachines <Citrix.DesktopUpdateManager.SDK.VirtualMachineCreation[]>

ADAccountName <string>

The domain-qualified AD Account name of the machine.

ADAccountSid <string>

The AD account SID of the machine account.

DiagnosticInformation <Citrix.MachineCreation.Sdk.ExceptionSurrogate[]>

A collection of handled error states which caused the provisioning to fail.

ExceptionType <string>

The type of exception this object represents

Message <string>

The exception message

Details <string>

The full exception content including stack trace

InnerException <Citrix.MachineCreation.Sdk.ExceptionSurrogate>

Information relating to any contributing error state

Status <string>

StatusAdditionalInformation <string>

VMId <string>

The virtual machine identifier in the hypervisor.

VMName <string>

The display name of the virtual machine in the hypervisor.

RemovedVirtualMachines <Citrix.DesktopUpdateManager.SDK.VirtualMachineCreation[]>

See FailedVirtualMachines for details of the object parameters.

ProgressEstimator

Gives an estimate of the number of virtual machines processed, averaging over virtual machines that were both partly and completely processed.

Notes

Only one long-running task for each provisioning scheme can be processed at a time.

This task still operates if the hosting unit or VMs in the hypervisor are missing. This removes the data from the Citrix Machine Creation Services, but the VMs remain in the hypervisor.

In the case of failure, the following errors can result.

Error Codes

JobCreationFailed

The requested task could not be started.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation. Communication with the database failed for

for various reasons.

WorkflowHostUnavailable

The task could not be started because the database connection is inactive.

CommunicationError

An error occurred while communicating with the service.

InvalidParameterCombination

Both PurgeJobOnSuccess and RunAsynchronously were specified. When running asynchronously, the cmdlet terminates before the job does, so it cannot clean up the completed job.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

The cmdlet is associated with a task of type RemoveVirtualMachine, and while active will move through the following operations (CurrentOperation field)

ValidatingInputs

RemovingVirtualMachines

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>,(Get-ProvVM -ProvisioningSchemeName XenPS) | Remove-ProvVM XenPS

TaskId               : cfb506a5-cc7e-4a49-ac7b-dd960029d0d3
Active               : False
Host                 : DDC
DateStarted          : 10/10/2012 16:39:45
Metadata             : {}
WorkflowStatus       : Completed
ProvisioningSchemeUid      : e1afc8fb-3f52-42ea-9a17-305fdb0b6ee4
ProvisioningSchemeName     : XenPS
TaskState            : Finished
```



```
TaskStateInformation        :
VirtualMachinesToRemoveCount : 2
RemovedVirtualMachines      : {XD\IP0001$, XD\IP0002$}
FailedVirtualMachines       : {}
VirtualMachinesRemovedCount  : 2
VirtualMachinesFailedCount   : 0
ProgressEstimator           : 2
Type                        : RemoveVirtualMachine
Status                      : Finished
CurrentOperation            :
TaskProgress                : 100
TaskExpectedCompletion      : 10/10/2012 16:39:50
LastUpdateTime              : 10/10/2012 16:39:50
ActiveElapsedTime           : 5
DateFinished                : 10/10/2012 16:39:50
TerminatingError            :
```

Remove all VMs from provisioning scheme XenPS

Rename-ProvScheme

Sep 10, 2014

Renames a provisioning scheme.

Syntax

Rename-ProvScheme [-ProvisioningSchemeName] <String> [-NewProvisioningSchemeName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Rename-ProvScheme -ProvisioningSchemeUid <Guid> [-NewProvisioningSchemeName] <String> [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to change the name of an existing provisioning scheme. The unique identifier for the provisioning scheme never changes after it has been created so, regardless of any name changes, the provisioning scheme can always be identified by its unique identifier.

Related topics

New-ProvScheme

Set-ProvScheme

Get-ProvScheme

Test-ProvSchemeNameAvailable

Parameters

-ProvisioningSchemeName<String>

The current name of the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ProvisioningSchemeUid<Guid>

The identifier for the provisioning scheme that is to be renamed.

Required?	true
Default Value	
Accept Pipeline Input?	false

-NewProvisioningSchemeName<String>

The new name for the provisioning scheme. This must be a name that is not being used by an existing provisioning scheme, and it must not contain any of the following characters \/;:#.*?=<>|[]()""'

Required?	true
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Defines whether or not the command returns a result showing the new state of the updated identity pool.

Required?	false
Default Value	true
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.ProvisioningScheme

This object provides details of the provisioning scheme and contains the following information:

ProvisioningSchemeUid

The unique identifier for the provisioning scheme.

ProvisioningSchemeName

The name of the provisioning scheme.

CpuCount

The numer of processors that VMs will be created with when using this scheme.

MemoryMB

The maximum amount of memory that VMs will be created with when using this scheme.

MasterImageVM

The path within the hosting unit provider to the VM or snapshot of which the scheme is currently using a copy.

MasterImageVMDate

The date and time that the copy of the VM image was made for the scheme.

IdentityPoolUid

The unique identifier of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

IdentityPoolName

The name of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

HostingUnitUid

The unique identifier of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme will use.

HostingUnitName

The name of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme will use.

CleanOnBoot

Indicates whether the VMs created are to be reset to a clean state on each boot.

TaskId

The identifier of any current task that is running for the provisioning scheme.

Metadata

The metadata for the provisioning scheme.

Notes

In the case of failure, the following errors can result.

Error Codes

ProvisioningSchemeNotFound

The specified provisioning scheme could not be located.

ProvisioningSchemeNameAlreadyExists

A provisioning scheme with the same name as the new provisioning scheme name already exists.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

ExceptionThrown

An unexpected error occurred. To locate more details, see the windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Rename-ProvScheme -provisioningSchemeName CurrentName -NewProvisioningSchemeName NewName
```

Renames a provisioning scheme from "currentName" to "NewName".

---------- EXAMPLE 2 ----------

```
C:\PS>Rename-ProvScheme -provisioningSchemeName CurrentName -NewProvisioningSchemeName NewName -PassThru


ProvisioningSchemeUid  : 7585f0de-192e-4847-a6d8-22713c3a2f42
ProvisioningSchemeName : NewName
CpuCount               : 1
MemoryMB               : 1024
MasterImageVM          : /Base.vm
MasterImageVMDate      : 17/05/2010 08:27:50
IdentityPoolUid        : 03743136-e43b-4a87-af74-ab71686b3c16
IdentityPoolName       : IdPool1
HostingUnitUid         : 01a4a008-8ce8-4165-ba9c-cdf15a6b0501
HostingUnitName        : XenHU
CleanOnBoot            : True
TaskId                 :
Metadata               : {}
```

Renames a provisioning scheme from "currentName" to "NewName" and displays the resulting state.

Reset-ProvServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the MachineCreation Service.

Syntax

```
Reset-ProvServiceGroupMembership [-ConfigServiceInstance] <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables you to reload MachineCreation Service access permissions and configuration service locations. The Reset-ProvServiceGroupMembership command must be run on at least one instance of the service type (Prov) after installation and registration with the configuration service. Without this operation, the MachineCreation services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-ProvServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Parameters

-ConfigServiceInstance<ServiceInstance[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.MachineCreation.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-ProvServiceGroupMembership command.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-ProvServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-ProvServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Set-ProvDBConnection

Sep 10, 2014

Configures a database connection for the MachineCreation Service.

Syntax

```
Set-ProvDBConnection [-DBConnection] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Configures a connection to a database in which the MachineCreation Service can store its state. The service will attempt to connect and start using the database immediately after the connection is configured. The database connection string is updated to the specified value regardless of whether it is valid or not. Specifying an invalid connection string prevents a service from functioning until the error is corrected.

After a connection is configured, you cannot alter it without first clearing it (by setting the connection to $null).

You do not need to configure a database connection to use this command.

Related topics

Get-ProvServiceStatus

Get-ProvDBConnection

Test-ProvDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the MachineCreation Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-ProvDBConnection command returns an object containing the status of the MachineCreation Service together with extra diagnostics information.

DBUnconfigured

The MachineCreation Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the MachineCreation Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the MachineCreation Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the MachineCreation Service currently in use is incompatible with the version of the MachineCreation Service schema on the database. Upgrade the MachineCreation Service to a more recent version.

DBOlderVersionThanService

The version of the MachineCreation Service schema on the database is incompatible with the version of the MachineCreation Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The MachineCreation Service is running and is connected to a database containing a valid schema.

Failed

The MachineCreation Service has failed.

Unknown

The status of the MachineCreation Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Set-ProvDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Configures a database connection string for the MachineCreation Service.

-------------------------- EXAMPLE 2 --------------------------

```
c:\PS>Set-ProvDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Configures an invalid database connection string for the MachineCreation Service.

Set-ProvScheme

Sep 10, 2014

Changes the parameter values for a provisioning scheme.

Syntax

Set-ProvScheme [-ProvisioningSchemeName] <String> [-VMCpuCount <Int32>] [-VMMemoryMB <Int32>] [-ServiceOffering <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvScheme [-ProvisioningSchemeName] <String> -IdentityPoolUid <Guid> [-VMCpuCount <Int32>] [-VMMemoryMB <Int32>] [-ServiceOffering <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvScheme [-ProvisioningSchemeName] <String> -IdentityPoolName <String> [-VMCpuCount <Int32>] [-VMMemoryMB <Int32>] [-ServiceOffering <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvScheme -ProvisioningSchemeUid <Guid> [-VMCpuCount <Int32>] [-VMMemoryMB <Int32>] [-ServiceOffering <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvScheme -ProvisioningSchemeUid <Guid> -IdentityPoolName <String> [-VMCpuCount <Int32>] [-VMMemoryMB <Int32>] [-ServiceOffering <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvScheme -ProvisioningSchemeUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <Int32>] [-VMMemoryMB <Int32>] [-ServiceOffering <String>] [-PassThru] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to update the parameters of an existing provisioning scheme.

This allows the following parameters to be updated:

Number of CPUs that will be used for VMs created from the provisioning scheme. Maximum amount of memory that will be used for VMs created from the provisioning scheme.

To change the name of the provisioning scheme see Rename-ProvScheme.

Related topics

New-ProvScheme

Remove-ProvScheme

Get-ProvScheme

Rename-ProvScheme

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme to be updated.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IdentityPoolUid<Guid>

The identifier of an identity pool to associate with the provisioning scheme, replacing the present one.

Required?	true
Default Value	
Accept Pipeline Input?	false

-IdentityPoolName<String>

The name of an identity pool to associate with the provisioning scheme, replacing the present one.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ProvisioningSchemeUid<Guid>

The identifier of the provisioning scheme to be updated.

Required?	true
Default Value	
Accept Pipeline Input?	false

-VMCpuCount<Int32>

The number of processors that virtual machines created from the provisioning scheme should use.

Required?	false
Default Value	
Accept Pipeline Input?	false

-VMMemoryMB<Int32>

The maximum amount of memory that virtual machines created from the provisioning scheme should use.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceOffering<String>

The name of the cloud service offering to use when creating machines.

Required?	false
Default Value	
Accept Pipeline Input?	false

-PassThru<SwitchParameter>

Returns the affected record. By default, this cmdlet does not generate any output.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.ProvisioningScheme

This object provides details of the provisioning scheme and contains the following information:

ProvisioningSchemeUid

ProvisioningSchemeName

The name of the provisioning scheme.

CpuCount

The numer of processors that VMs will be created with when using this scheme.

MemoryMB

The maximum amount of memory that VMs will be created with when using this scheme.

MasterImageVM

The path within the hosting unit provider to the VM or snapshot of which the scheme is currently using a copy.

MasterImageVMDate

The date and time that the copy of the VM image was made for the scheme.

IdentityPoolUid

The unique identifier of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

IdentityPoolName

The name of the identity pool (from the ADIdentity PowerShell snap-in) that the scheme uses.

HostingUnitUid

The unique identifier of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme will use.

HostingUnitName

The name of the hosting unit (from the Hosting Unit PowerShell snap-in) that the new provisioning scheme will use.

CleanOnBoot

Indicates whether the VMs created are to be reset to a clean state on each boot.

TaskId

The identifier of any current task that is running for the provisioning scheme.

Notes

In the case of failure, the following errors can result.

Error Codes

ProvisioningSchemeNotFound

The specified provisioning scheme could not be located.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

HostingUnitNotFound

The hosting unit referenced by the provisioning scheme could not be resolved

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> Set-ProvScheme -ProvisioningSchemeName MyScheme -VMCpuCount 2
```

Updates a provisioning scheme called "MyScheme" to use two processors on the VMs that are created from the provisioning scheme.

Set-ProvSchemeMetadata

Sep 10, 2014

Adds or updates metadata on the given ProvisioningScheme.

Syntax

Set-ProvSchemeMetadata [-ProvisioningSchemeUid] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvSchemeMetadata [-ProvisioningSchemeUid] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvSchemeMetadata [-ProvisioningSchemeName] <String> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvSchemeMetadata [-ProvisioningSchemeName] <String> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvSchemeMetadata [-InputObject] <ProvisioningScheme[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvSchemeMetadata [-InputObject] <ProvisioningScheme[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored against given ProvisioningScheme objects.

Related topics

Add-ProvSchemeMetadata

Remove-ProvSchemeMetadata

Parameters

-ProvisioningSchemeUid<Guid>

Id of the ProvisioningScheme

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-ProvisioningSchemeName<String>

Name of the ProvisioningScheme

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<ProvisioningScheme[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the ProvisioningScheme specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()'"

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-ProvSchemeMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-ProvSchemeMetadata -ProvisioningSchemeUid 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                            -----
        property                           value
```

Add metadata with a name of 'property' and a value of 'value' to the ProvisioningScheme with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-ProvServiceConfigurationData

Sep 10, 2014

Sets the value for the given key in the service configuration data.

Syntax

Set-ProvServiceConfigurationData [-Name] <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability for additional custom data to be stored for the MachineCreation Service.

Related topics

Remove-ProvServiceConfigurationData

Get-ProvServiceConfigurationData

Parameters

-Name<String>

Specifies the key name of the metadata to be added. The key must be unique.

The Name cannot contain any of the following characters \/;:#.*?=<>|[]()'"""

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the name. If the name already exists, its value is updated.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create

high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.MachineCreation.Sdk.ServiceConfigurationData

Set-ProvServiceConfigurationData returns an object containing the new definition of the configuration.

Name <string>

Specifies the name for the item of data.

Value <string>

Specifies the value of the data.

Notes

In the case of failure the following errors can be produced.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

An error occurred while communicating with the service.

ExceptionThrown

An unexpected error occurred. To locate more details see the Windows event logs on the controller being used, or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Set-ProvServiceConfigurationData -Name "customProperty1" -Value "value2"

Name                 Value
--------             -----
customProperty1      value2
```

Set data with a name of 'customProperty1' and value of 'value2' to the service configuration.

Set-ProvServiceMetadata

Sep 10, 2014

Adds or updates metadata on the given Service.

Syntax

Set-ProvServiceMetadata [-ServiceHostId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvServiceMetadata [-InputObject] <Service[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Allows you to store additional custom data against given Service objects.

Related topics

Remove-ProvServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Service specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-ProvServiceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Set-ProvServiceMetadata -ServiceHostId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Service with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-ProvTaskMetadata

Sep 10, 2014

Adds or updates metadata on the given Task.

Syntax

Set-ProvTaskMetadata [-TaskId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvTaskMetadata [-TaskId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvTaskMetadata [-InputObject] <Task[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-ProvTaskMetadata [-InputObject] <Task[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Use this cmdlet to store additional custom data against given Task objects.

Related topics

Add-ProvTaskMetadata

Remove-ProvTaskMetadata

Get-ProvTask

Stop-ProvTask

Remove-ProvTask

Switch-ProvTask

Parameters

-TaskId<Guid>

Id of the Task

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Task[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Task specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-ProvTaskMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can result.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-ProvTaskMetadata -TaskId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Task with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Stop-ProvTask

Sep 10, 2014

Stops currently running MachineCreation Service tasks.

Syntax

```
Stop-ProvTask [-TaskId] <Guid> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables tasks currently running in the MachineCreation Service to be stopped. Once stopped, tasks cannot be restarted.

Related topics

Get-ProvTask

Remove-ProvTask

Switch-ProvTask

Parameters

-TaskId<Guid>

Specifies the identifier for the task to be stopped.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.Management.Automation.PSObject Objects containing the TaskId parameter can be piped to the Stop-ProvTask command.

Notes

If the command fails, the following errors can result.

Error Codes

InvalidWorkflow

The specified task could not be found.

InvalidWorkflowHost

The specified task is executing on a different server.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

DatabaseError

There was a problem communicating with the database.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ProvTask -active $true | Stop-ProvTask
Success
```

Terminate all tasks currently executing on the MachineCreation Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Stop-ProvTask -TaskId bd52e688-e40d-4790-83de-9f7633481454
Success
```

Terminate the named task executing on the MachineCreation Service.

Switch-ProvTask

Sep 10, 2014

Moves all MachineCreation Service tasks from the current execution host to another.

Syntax

```
Switch-ProvTask [-Host2] <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Enables tasks running within the MachineCreation Service to be moved from one execution host to a different host.

Tasks can only execute on a single host. If the host is removed from a deployment, the tasks cannot continue to execute. These 'orphaned' tasks can be moved to a different host within the deployment so that they can continue to execute. All tasks must be moved; there is no mechanism to move individual tasks. Run the Switch-ProvTask command against the host to which the tasks are to be moved; that is, if you are not running the command directly on the host, use the AdminAddress parameter to specify the host to which tasks will be moved.

Related topics

Get-ProvTask

Stop-ProvTask

Remove-ProvTask

Parameters

-Host2<String>

Specifies the host from which the tasks should be removed.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false

Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can result.

Error Codes

PartialData

Only a subset of the requested data was returned.

NoOp

The operation was successful but had no effect.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Switch-ProvTask -Host CRASHED
Success
```

Transfer the execution of tasks that had been executing on the MachineCreation Service instance on host CRASHED to the local instance.

Test-ProvDBConnection

Sep 10, 2014

Tests a database connection for the MachineCreation Service.

Syntax

```
Test-ProvDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Tests a connection to the database in which the MachineCreation Service can store its state. The service will attempt to connect to the database without affecting the current connection to the database.

You do not have to clear the connection to use this command.

Related topics

Get-ProvServiceStatus

Get-ProvDBConnection

Set-ProvDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the MachineCreation Service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-ProvDBConnection command returns an object containing the status of the MachineCreation Service if the connection string of the specified data store were to be set to the string being tested, together with extra diagnostics information for the specified connection string.

DBRejectedConnection

The database rejected the logon attempt from the MachineCreation Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the MachineCreation Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the MachineCreation Service currently in use is incompatible with the version of the MachineCreation Service schema on the database. Upgrade the MachineCreation Service to a more recent version.

DBOlderVersionThanService

The version of the MachineCreation Service schema on the database is incompatible with the version of the MachineCreation Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Set-ProvDBConnection command would succeed if it were executed with the supplied connection string.

Failed

The MachineCreation Service has failed.

Unknown

The status of the MachineCreation Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Test-ProvDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"
```


OK
Tests a database connection string for the MachineCreation Service.

---------- EXAMPLE 2 ----------

c:\PS>Test-ProvDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
Tests an invalid database connection string for the MachineCreation Service.

Test-ProvSchemeNameAvailable

Sep 10, 2014

Checks to ensure that the proposed name for a provisioning scheme is unused.

Syntax

```
Test-ProvSchemeNameAvailable -ProvisioningSchemeName <String[]> [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Checks to ensure that the proposed name for a provisioning scheme is unused. This check is done without regard for scoping of existing provisioning schemes, so the names of inaccessible schemes are also checked.

Related topics

New-ProvScheme

Rename-ProvScheme

Parameters

-ProvisioningSchemeName<String[]>

The name or names of the provisioning scheme(s) to be tested.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

NameAvailability

Pairs of name and the availability of the name

Notes

In the case of failure, the following errors can result.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
Test-ProvSchemeNameAvailable -ProvisioningSchemeName $NewSchemeName
```

This tests whether the value of $NewSchemeName is unique or not, and can be used to create a new provisioning scheme or rename an existing one without failing. True is returned if the name is good.

Unlock-ProvScheme

Sep 10, 2014

Unlocks a Provisioning Scheme.

Syntax

Unlock-ProvScheme [-ProvisioningSchemeName] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Unlock-ProvScheme -ProvisioningSchemeUid <Guid> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Provides the ability to unlock a provisioning scheme that has the Id of a failed Task still associated with it. This allows another long-running task to operate on that scheme. The cmdlet will not unlock a scheme with a task still marked as being active. Use Stop-ProvTask (or, if the task is registered with a failed server, Switch-ProvTask and Stop-ProvTask) to stop any active task first.

Related topics

Get-ProvScheme

Stop-ProvTask

Parameters

-ProvisioningSchemeName<String>

The name of the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeUid<Guid>

The unique identifier of the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

In the case of failure, the following errors can result.

Error Codes

ProvisioningSchemeNotFound

The specified provisioning scheme could not be located.

NoOp

The specified provisioning scheme had no task object associated.

TaskActive

The task object associated with the provisioning scheme is still active.

DatabaseError

An error occurred in the service while attempting a database operation.

CouldNotQuueryDatabase

The query required to get the database was not defined.

CommunicationError

An error occurred while communicating with the service.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Unlock-ProvScheme -provisioningSchemeName MyScheme
```

Unlocks the provisioning scheme 'MyScheme'.

Unlock-ProvVM

Sep 10, 2014

Unlocks a VM.

Syntax

```
Unlock-ProvVM [-VMID] <String[]> -ProvisioningSchemeName <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Unlock-ProvVM [-VMID] <String[]> -ProvisioningSchemeUid <Guid> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to unlock a virtual machine.

Related topics

Get-ProvVM

Lock-ProvVM

Parameters

-VMID<String[]>

The virtual machine Id (hypervisor context)

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeName<String>

The name of the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-ProvisioningSchemeUid<Guid>

The unique identifier of the provisioning scheme.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller that the PowerShell snap-in connects to. You can provide this as a host name or an IP address.

Required?	false
Default Value	LocalHost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.MachineCreation.Sdk.ProvisionedVirtualMachine You can pipe an object containing a parameter called 'VMId' and 'ProvisioningSchemeName' to Lock-ProvVM

Notes

In the case of failure, the following errors can result.

Error Codes

VMDoesNotExist

The specified VM cannot be located.

VMAlreadyUnLocked

The VM is already unlocked.

VMDoesNotExistForProvisioningScheme

The specified VM does exist in the hypervisor, but is not part of the specified provisioning scheme.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for

for various reasons.

CommunicationError

An error occurred while communicating with the service.

PermissionDenied

The user does not have administrative rights to perform this operation.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error

ExceptionThrown

An unexpected error occurred. To locate more details, see the Windows event logs on the controller being used or examine the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Unlock-ProvVM -provisioningSchemeName MyScheme -VMId  bc79802c-ba6e-8de8-99e9-4c35d7ad24b4
```

Unlocks the VM with the Id 'bc79802c-ba6e-8de8-99e9-4c35d7ad24b4' in the provisioning scheme 'MyScheme'.

---------- EXAMPLE 2 ----------

```
C:\PS>Get-ProvVM -provisioningSchemeName MyScheme | Unlock-ProvVM
```

Unlocks all the VMs in the provisioning scheme 'MyScheme'.

---------- EXAMPLE 3 ----------

```
C:\PS>Get-ProvVM -Locked $True | Unlock-ProvVM
```

Unlocks all the VMs that are currently locked.

Citrix.Monitor.Admin.V1

Sep 10, 2014

Overview

Name	Description
MonitorMonitorSnapin	The Monitor Service PowerShell snap-in provides administrative functions for the Monitor Service.
Monitor Filtering	Describes the common filtering options for XenDesktop cmdlets.

Cmdlets

Name	Description
Get-MonitorConfiguration	Gets the configuration settings currently being used by the Monitor Service.
Get-MonitorDataStore	Gets details for each of the Monitor data stores.
Get-MonitorDBConnection	Gets the database string for the specified data store used by the Monitor Service.
Get-MonitorDBSchema	Gets a script that creates the Monitor Service database schema for the specified data store.
Get-MonitorDBVersionChangeScript	Gets a script that updates the Monitor Service database schema.
Get-MonitorInstalledDBVersion	Gets a list of all available database schema versions for the Monitor Service.
Get-MonitorService	Gets the service record entries for the Monitor Service.
Get-MonitorServiceAddedCapability	Gets any added capabilities for the Monitor Service on the controller.
Get-MonitorServiceInstance	Gets the service instance entries for the Monitor Service.
Get-MonitorServiceStatus	Gets the current status of the Monitor Service on the controller.
Remove-MonitorServiceMetadata	Removes metadata from the given Service.
Reset-MonitorDataStore	Refreshes the database string currently being used by the Monitor service.

Name	Description
Reset-MonitorServiceGroupMembership	Reloads the access permissions and configuration service locations for the Monitor Service.
Set-MonitorConfiguration	Sets configuration settings that are used by the Monitor Service.
Set-MonitorDBConnection	Configures a database connection for the Monitor Service.
Set-MonitorServiceMetadata	Adds or updates metadata on the given Service.
Test-MonitorDBConnection	Tests a database connection for the Monitor Service.

about_MonitorMonitorSnapin

Sep 10, 2014

TOPIC

about_MonitorMonitorSnapin

SHORT DESCRIPTION

The Monitor Service PowerShell snap-in provides administrative functions for the Monitor Service.

COMMAND PREFIX

All commands in this snap-in have the noun prefixed with 'Monitor'.

LONG DESCRIPTION

The Monitor Service PowerShell snap-in enables both local and remote administration of the Monitor service. It provides

facilities to query the Monitor service configuration settings and to modify those settings. It also provides the

standard set of XenDesktop service cmdlets.

about_Monitor_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```

retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

A120901
B220000
...

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

Get-MonitorConfiguration

Sep 10, 2014

Gets the configuration settings currently being used by the Monitor Service.

Syntax

```
Get-MonitorConfiguration [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the configuration currently being used by the Monitor Service.

A site database connection must be configured for this command to be used.

Related topics

Set-MonitorConfiguration

Parameters

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Get-MonitorConfiguration returns the configuration settings.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-MonitorConfiguration
```

Gets the current configuration for the Monitor Service.

Get-MonitorDataStore

Sep 10, 2014

Gets details for each of the Monitor data stores.

Syntax

```
Get-MonitorDataStore [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns an object for each of the Monitor data stores describing the connection string, data store name, db type, provider, schema name, and DB status.

A database connection must be configured in order for this command to be used if the service has a secondary data store. This is not required for the site data store.

Related topics

Reset-MonitorDataStore

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Monitor.Sdk.DataStoreConfiguration

An object describing the connection string, data store name, database type, provider, schema name and database status.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-MonitorDataStore

ConnectionString : Server=.\SQLEXPRESS;Initial Catalog = databaseName; Integrated Security = True
DataStore        : Site
DatabaseType     : SqlServer
Provider         : MSSQL
SchemaName       : MonitorSiteSchema
Status           : OK

ConnectionString :
DataStore        : Secondary
DatabaseType     : SqlServer
Provider         : MSSQL
SchemaName       : MonitorSecondarySchema
Status           : DBUnconfigured
```

Get the database connection string for the Monitor Service.

Get-MonitorDBConnection

Sep 10, 2014

Gets the database string for the specified data store used by the Monitor Service.

Syntax

```
Get-MonitorDBConnection [[-DataStore] <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the database connection string for the specified data store.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

Related topics

Get-MonitorServiceStatus

Get-MonitorDataStore

Set-MonitorDBConnection

Test-MonitorDBConnection

Parameters

-DataStore<String>

Specifies the logical name of the data store for the Monitor Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false
Default Value	Site
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

system.string

The database connection string configured for the Monitor Service.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the Monitor Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-MonitorDBConnection

Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True
```

Get the database connection string for the Monitor Service.

Get-MonitorDBSchema

Sep 10, 2014

Gets a script that creates the Monitor Service database schema for the specified data store.

Syntax

Get-MonitorDBSchema [-DatabaseName <String>] [-ServiceGroupName <String>] [-ScriptType <ScriptTypes>] [-LocalDatabase] [-Sid <String>] [-DataStore <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets SQL scripts that can be used to create a new Monitor Service database schema, add a new Monitor Service to an existing site, remove a Monitor Service from a site, or create a database server logon for a Monitor Service. If no Sid parameter is provided, the scripts obtained relate to the currently selected Monitor Service instance, otherwise the scripts relate to Monitor Service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied. The current service instance is that on the local machine, or that explicitly specified by the last usage of the -AdminAddress parameter to a Monitor SDK cmdlet. The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured. The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SMDCMD mode'. The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to Monitor Service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to Monitor Service roles

If ScriptType is Evict, the returned script contains:

o Removal of Monitor Service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database. You do not need to configure a database before using this command.

Related topics

Get-MonitorDataStore

Set-MonitorDBConnection

Parameters

-DatabaseName<String>

Specifies the name of the database for which the schema will be generated.

Required?	false
Default Value	

Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the Monitor services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<ScriptTypes>

Specifies the type of database script returned. Available script types are:

Database

Returns a full database script that can be used to create a database schema for the Monitor Service in a database instance that does not already contain a schema for this service. The DatabaseName and ServiceGroupName parameters must be specified to create a script of this type.

Instance

Returns a permissions script that can be used to add further Monitor services to an existing database instance that already contains the full Monitor service schema, associating the services to the Service Group. The Sid parameter can optionally be specified to create a script of this type.

Login

Returns a database logon script that can be used to add the required logon accounts to an existing database instance that contains the Monitor Service schema. This is used primarily when creating a mirrored database environment. The DatabaseName parameter must be specified to create a script of this type.

Evict

Returns a script that can be used to remove the specified Monitor Service from the database entirely. The DatabaseName and Sid parameters must be specified to create a script of this type.

Required?	false
Default Value	Database
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for Monitor services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Sid<String>

Specifies the SID of the controller on which the Monitor Service instance to remove from the database is running.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-DataStore<String>

Specifies the logical name of the data store for the Monitor Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false
Default Value	Site
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.string

A string containing the required SQL script for application to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-MonitorDBSchema -DatabaseName MyDB -ServiceGroupName  MyServiceGroup > c:\MonitorSchema.sql
```

Get the full database schema for site data store of the Monitor Service and copy it to a file called 'c:\MonitorSchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a Monitor Service site schema.

-------------------------- EXAMPLE 2 --------------------------

```
c:\PS>Get-MonitorDBSchema -DatabaseName MyDB -scriptType Login > c:\MonitorLogins.sql
```

Get the logon scripts for the Monitor Service.

-------------------------- EXAMPLE 3 --------------------------

```
c:\PS>Get-MonitorDBSchema -DatabaseName MyDB -ServiceGroupName MyServiceGroup -DataStore Secondary > c:\MonitorSchema.sql
```

Get the full database schema for the secondary data store of the Monitor Service and copy it to a file called 'c:\MonitorSecondarySchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a Monitor Service secondary schema.

Get-MonitorDBVersionChangeScript

Sep 10, 2014

Gets a script that updates the Monitor Service database schema.

Syntax

```
Get-MonitorDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-DataStore <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a database script that can be used to upgrade or downgrade the site or secondary schema for the Monitor Service from the current schema version to a different version.

Related topics

Get-MonitorInstalledDBVersion

Parameters

-DatabaseName<String>

Specifies the name of the database instance to which the update applies.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

Specifies the version of the database you want to update to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-DataStore<String>

Specifies the logical name of the data store for the Monitor Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false
Default Value	Site
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

A PSObject containing the required SQL script for application to a database.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any Monitor services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-MonitorServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Monitor Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $update = Get-MonitorDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-MonitorInstalledDBVersion

Sep 10, 2014

Gets a list of all available database schema versions for the Monitor Service.

Syntax

```
Get-MonitorInstalledDBVersion [-Upgrade] [-Downgrade] [-DataStore <String>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the current version of the Monitor Service database schema, if no flags are set, otherwise returns versions for which upgrade or downgrade scripts are available and have been stored in the database.

Related topics

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DataStore<String>

Specifies the database connection logical name the schema script should be returned for. The parameter is optional.

Required?	false
Default Value	

Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Version

The Get-MonitorInstalledDbVersion command returns objects containing the new definition of the Monitor Service database schema version.

Major <Integer>

Minor <Integer>

Build <Integer>

Revision <Integer>

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Monitor Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-MonitorInstalledDBVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      6      0      0
```

Get the currently installed version of the Monitor Service database schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-MonitorInstalledDBVersion -Upgrade

Major  Minor  Build  Revision
-----  -----  -----  --------
6      0      0      0
```

Get the versions of the Monitor Service database schema for which upgrade scripts are supplied.

Get-MonitorService

Sep 10, 2014

Gets the service record entries for the Monitor Service.

Syntax

Get-MonitorService [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns instances of the Monitor Service that the service publishes. The service records contain account security identifier information that can be used to remove each service from the database.

A database connection for the service is required to use this command.

Related topics

Parameters

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Monitor_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Monitor_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Monitor.Sdk.Service

The Get-MonitorServiceInstance command returns an object containing the following properties.

Uid <Integer>

Specifies the unique identifier for the service in the group. The unique identifier is an index number.

ServiceHostId <Guid>

Specifies the unique identifier for the service instance.

DNSName <String>

Specifies the domain name of the host on which the service runs.

MachineName <String>

Specifies the short name of the host on which the service runs.

CurrentState <Citrix.Fma.Sdk.ServiceCore.ServiceState>

Specifies whether the service is running, started but inactive, stopped, or failed.

LastStartTime <DateTime>

Specifies the date and time at which the service was last restarted.

LastActivityTime <DateTime>

Specifies the date and time at which the service was last stopped or restarted.

OSType

Specifies the operating system installed on the host on which the service runs.

OSVersion

Specifies the version of the operating system installed on the host on which the service runs.

ServiceVersion

Specifies the version number of the service instance. The version number is a string that reflects the full build version of the service.

DatabaseUserName <string>

Specifies for the service instance the Active Directory account name with permissions to access the database. This will be either the machine account or, if the database is running on a controller, the NetworkService account.

Sid <string>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

ActiveSiteServices <string[]>

Specifies the names of active site services currently running in the service. Site services are components that perform long-running background processing in some services. This field is empty for services that do not contain site services.

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-MonitorService

Uid             : 1
ServiceHostId   : aef6f464-f1ee-4042-a523-66982e0cecd0
DNSName         : MyServer.company.com
MachineName     : MYSERVER
CurrentState    : On
LastStartTime   : 04/04/2011 15:25:38
LastActivityTime : 04/04/2011 15:33:39
OSType          : Win32NT
OSVersion       : 6.1.7600.0
ServiceVersion  : 5.1.0.0
DatabaseUserName : NT AUTHORITY\NETWORK SERVICE
SID             : S-1-5-21-2316621082-1546847349-2782505528-1165
ActiveSiteServices : {MySiteService1, MySiteService2...}
```

Get all the instances of the Monitor Service running in the current service group.

Get-MonitorServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the Monitor Service on the controller.

Syntax

```
Get-MonitorServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the Monitor Service on the controller to be detected.

You do not need to configure a database connection before using this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-MonitorServiceAddedCapability
```

Get the added capabilities of the Monitor Service.

Get-MonitorServiceInstance

Sep 10, 2014

Gets the service instance entries for the Monitor Service.

Syntax

```
Get-MonitorServiceInstance [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns service interfaces published by the instance of the Monitor Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Monitor.Sdk.ServiceInstance

The Get-MonitorServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a

central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

Specifies the service instance type. For this service, the service instance type is always Monitor.

Address

Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

SDK - for PowerShell operations

InterService - for operations between different services

Peer - for communications between services of the same type

Metadata <Citrix.Monitor.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-MonitorServiceInstance

Address          : http://MyServer.com:80/Citrix/Monitor
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         :
MetadataMap      :
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName  : MyServiceGroup
ServiceGroupUid   : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType      : Monitor
Version          : 1

Address          : http://MyServer.com:80/Citrix/Monitor/IServiceApi
Binding          : wcf_HTTP_kerb
InterfaceType    : InterService
Metadata         :
MetadataMap      :
```



```
ServiceAccount     : ENG\MyAccount
ServiceAccountSid  : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName   : MyServiceGroup
ServiceGroupUid    : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType        : Monitor
Version            : 1
```

Get all instances of the Monitor Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-MonitorServiceStatus

Sep 10, 2014

Gets the current status of the Monitor Service on the controller.

Syntax

```
Get-MonitorServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the Monitor Service on the controller to be monitored. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured.

Related topics

Get-MonitorDataStore

Set-MonitorDBConnection

Test-MonitorDBConnection

Get-MonitorDBConnection

Get-MonitorDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-MonitorServiceStatus command returns an object containing the status of the Monitor Service together with extra diagnostics information.

DBUnconfigured

The Monitor Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the Monitor Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Monitor Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Monitor Service currently in use is incompatible with the version of the Monitor Service schema on the database. Upgrade the Monitor Service to a more recent version.

DBOlderVersionThanService

The version of the Monitor Service schema on the database is incompatible with the version of the Monitor Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Monitor Service is running and is connected to a database containing a valid schema.

Failed

The Monitor Service has failed.

Unknown

(0) The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-MonitorServiceStatus
```

```
DBUnconfigured
```

Get the current status of the Monitor Service.

Remove-MonitorServiceMetadata

Sep 10, 2014

Removes metadata from the given Service.

Syntax

```
Remove-MonitorServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-MonitorServiceMetadata [-ServiceHostId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-MonitorServiceMetadata [-InputObject] <Service[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-MonitorServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Service.

Related topics

Set-MonitorServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- **EXAMPLE 1** ----------

```
c:\PS>Get-MonitorService | % { Remove-MonitorServiceMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Service objects.

Reset-MonitorDataStore

Sep 10, 2014

Refreshes the database string currently being used by the Monitor service.

Syntax

```
Reset-MonitorDataStore [-DataStore] <String> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Returns the string for the database connection currently being used by the Monitor Service. Can only be called for secondary data stores.

There is no requirement for a database connection to be configured in order for this command to be used.

Related topics

Get-MonitorDataStore

Parameters

-DataStore<String>

Specifies the database connection logical name to be used by the Monitor Service. Can be either be 'Site' or the logical name of the secondary data store. Specifying the site data store will display an error because this operation is not supported for site data stores.

Required?	true
Default Value	Site
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Monitor.Sdk.ServiceStatus

The status of the specified data store.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Reset-MonitorDataStore -DataStore Secondary
OK
```

Refresh the database connection string for the Monitor Service.

Reset-MonitorServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the Monitor Service.

Syntax

```
Reset-MonitorServiceGroupMembership [-ConfigServiceInstance] <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables you to reload Monitor Service access permissions and configuration service locations. The Reset-MonitorServiceGroupMembership command must be run on at least one instance of the service type (Monitor) after installation and registration with the configuration service. Without this operation, the Monitor services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-MonitorServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Parameters

-ConfigServiceInstance<ServiceInstance[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.Monitor.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-MonitorServiceGroupMembership command.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-MonitorServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-MonitorServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Set-MonitorConfiguration

Sep 10, 2014

Sets configuration settings that are used by the Monitor Service.

Syntax

```
Set-MonitorConfiguration [-GroomSessionsRetentionDays <Int32>] [-GroomFailuresRetentionDays <Int32>] [-GroomLoadIndexesRetentionDays <Int32>] [-GroomDeletedRetentionDays <Int32>] [-GroomSummariesRetentionDays <Int32>] [-GroomMachineHotfixLogRetentionDays <Int32>] [-GroomMinuteRetentionDays <Int32>] [-DataCollectionEnabled <Boolean>] [-FullPollStartHour <Int32>] [-ResolutionPollTimeHours <Int32>] [-SyncPollTimeHours <Int32>] [-DetailedSqlOutputEnabled <Boolean>] [-CollectHotfixDataEnabled <Boolean>] [-GroomApplicationInstanceRetentionDays <Int32>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Sets the configuration settings used by the Monitor Service. Use these settings to modify the behavior of the service.

A database connection need not be configured for this command to be used.

> ### Note
>
> For parameters whose default values depend on the product edition, as noted here, the values of these parameters are set to the new default values when the edition is changed.

Related topics

Get-MonitorConfiguration

Parameters

-GroomSessionsRetentionDays<Int32>

Determines how many days to keep Session and Connection records after the Session is terminated.

Required?	false
Default Value	7 for non-platinum, 90 for platinum.
Accept Pipeline Input?	false

-GroomFailuresRetentionDays<Int32>

Determines how many days to keep MachineFailureLog and ConnectionFailureLog records after these are created.

Required?	false
Default Value	7 for non-platinum, 90 for platinum.
Accept Pipeline Input?	false

-GroomLoadIndexesRetentionDays<Int32>

Determines how many days to keep LoadIndex records after these are created.

Required?	false
Default Value	7 for non-platinum, 90 for platinum.
Accept Pipeline Input?	false

-GroomDeletedRetentionDays<Int32>

Determines how many days to keep Machine, Catalog, DesktopGroup and Hypervisor entities around that have a LifecycleState of 'Deleted'. This also deletes any related Session, Connection, Summary, Failure or LoadIndex records.

Required?	false
Default Value	7 for non-platinum, 90 for platinum.
Accept Pipeline Input?	false

-GroomSummariesRetentionDays<Int32>

Determines how many days to keep DesktopGroupSummary, FailureLogSummary and LoadIndexSummary records at the daily granularity.

Required?	false
Default Value	7 for non-platinum, 90 for platinum.
Accept Pipeline Input?	false

-GroomMachineHotfixLogRetentionDays<Int32>

Determines how many days to keep Machine-Hotfix history records at the daily granularity.

Required?	false
Default Value	90
Accept Pipeline Input?	false

-GroomMinuteRetentionDays<Int32>

Determines how many days to keep minute data.

Required?	false
Default Value	3
Accept Pipeline Input?	false

-DataCollectionEnabled<Boolean>

Starts / stops data collection. Stopping data collection turns off polling, and does not persist operational event data to the database.

Required?	false
Default Value	True
Accept Pipeline Input?	false

-FullPollStartHour<Int32>

Hour of day when Full Poll should begin.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ResolutionPollTimeHours<Int32>

Start time for the Resolution Poll worker.

Required?	false

Default Value	
Accept Pipeline Input?	false

-SyncPollTimeHours<Int32>

Start time for Sync Poll worker.

Required?	false
Default Value	
Accept Pipeline Input?	false

-DetailedSqlOutputEnabled<Boolean>

Determines if the SqlLog should be enabled to send SQL statements to the CDF Trace

Required?	false
Default Value	False
Accept Pipeline Input?	false

-CollectHotfixDataEnabled<Boolean>

This setting determines if the hotfix inventory data should be collected and stored in the database or if it should be thrown away.

Required?	false
Default Value	
Accept Pipeline Input?	false

-GroomApplicationInstanceRetentionDays<Int32>

Required?	false
Default Value	

Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Examples

---------- EXAMPLE 1 ----------

```
C:\PS>Set-MonitorConfiguration -GroomSessionsRetentionDays 5 -GroomFailuresRetentionDays 4 ...
```

Updates the settings in the site database with the newly specified values.

Set-MonitorDBConnection

Sep 10, 2014

Configures a database connection for the Monitor Service.

Syntax

```
Set-MonitorDBConnection [-DBConnection] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [[-DataStore] <String>] [<CommonParameters>]
```

Detailed Description

Configures a connection to a database in which the Monitor Service can store its state. The service will attempt to connect and start using the database immediately after the connection is configured. The database connection string is updated to the specified value regardless of whether it is valid or not. Specifying an invalid connection string prevents a service from functioning until the error is corrected.

After a connection is configured, you cannot alter it without first clearing it (by setting the connection to $null).

You do not need to configure a database connection to use this command.

Related topics

Get-MonitorServiceStatus

Get-MonitorDBConnection

Test-MonitorDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the Monitor Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

-DataStore<String>

Specifies the logical name of the data store for the Monitor Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false
Default Value	Site
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-MonitorDBConnection command returns an object containing the status of the Monitor Service together with extra diagnostics information.

DBUnconfigured

The Monitor Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the Monitor Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Monitor Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Monitor Service currently in use is incompatible with the version of the Monitor Service schema on the database. Upgrade the Monitor Service to a more recent version.

DBOlderVersionThanService

The version of the Monitor Service schema on the database is incompatible with the version of the Monitor Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Monitor Service is running and is connected to a database containing a valid schema.

Failed

The Monitor Service has failed.

Unknown

The status of the Monitor Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

DatabaseError

An error occurred in the service while attempting a database operation.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Set-MonitorDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Configures a database connection string for the Monitor Service.

-------------------------- EXAMPLE 2 --------------------------

```
c:\PS>Set-MonitorDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Configures an invalid database connection string for the Monitor Service.

Set-MonitorServiceMetadata

Sep 10, 2014

Adds or updates metadata on the given Service.

Syntax

Set-MonitorServiceMetadata [-ServiceHostId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-MonitorServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-MonitorServiceMetadata [-InputObject] <Service[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-MonitorServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Allows you to store additional custom data against given Service objects.

Related topics

Remove-MonitorServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Service specified. The property cannot contain any of the following characters \/:;#.*?=<>|[]()"'

Required?	true

Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-MonitorServiceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------


```
c:\PS>Set-MonitorServiceMetadata -ServiceHostId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Service with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Test-MonitorDBConnection

Sep 10, 2014

Tests a database connection for the Monitor Service.

Syntax

```
Test-MonitorDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [[-DataStore] <String>]
[<CommonParameters>]
```

Detailed Description

Tests a connection to the database in which the Monitor Service can store its state. The service will attempt to connect to the database without affecting the current connection to the database.

You do not have to clear the connection to use this command.

Related topics

Get-MonitorServiceStatus

Get-MonitorDBConnection

Set-MonitorDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the Monitor Service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

-DataStore<String>

Specifies the logical name of the data store for the Monitor Service. Can be either be 'Site' or the logical name of the secondary data store.

Required?	false

Default Value	Site
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-MonitorDBConnection command returns an object containing the status of the Monitor Service if the connection string of the specified data store were to be set to the string being tested, together with extra diagnostics information for the specified connection string.

DBRejectedConnection

The database rejected the logon attempt from the Monitor Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Monitor Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Monitor Service currently in use is incompatible with the version of the Monitor Service schema on the database. Upgrade the Monitor Service to a more recent version.

DBOlderVersionThanService

The version of the Monitor Service schema on the database is incompatible with the version of the Monitor Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Set-MonitorDBConnection command would succeed if it were executed with the supplied connection string.

Failed

The Monitor Service has failed.

Unknown

The status of the Monitor Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseError

An error occurred in the service while attempting a database operation.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Test-MonitorDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Tests a database connection string for the Monitor Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Test-MonitorDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Tests an invalid database connection string for the Monitor Service.

Citrix.Storefront.Admin.V1

Sep 10, 2014

Overview

Name	Description
SfStorefrontSnapin	This service short description
Sf Filtering	Describes the common filtering options for XenDesktop cmdlets.

Cmdlets

Name	Description
Add-SfServerToCluster	Adds a new server to an existing cluster.
Add-SfStorefrontAddress	Modifies a StoreFront address configuration by adding an additional StoreFront address to it.
Get-SfCluster	Gets all Storefront clusters present in the site.
Get-SfDBConnection	Gets the database string for the specified data store used by the Storefront Service.
Get-SfDBSchema	Gets a script that creates the Storefront Service database schema for the specified data store.
Get-SfDBVersionChangeScript	Gets a script that updates the Storefront Service database schema.
Get-SfInstalledDBVersion	Gets a list of all available database schema versions for the Storefront Service.
Get-SfIsStorefrontInstalled	Tells whether StoreFront Services and Privileged Service are installed.
Get-SfService	Gets the service record entries for the Storefront Service.
Get-SfServiceAddedCapability	Gets any added capabilities for the Storefront Service on the controller.
Get-SfServiceInstance	Gets the service instance entries for the Storefront Service.
Get-SfServiceStatus	Gets the current status of the Storefront Service on the controller.

Name	Description
Get-SfStorefrontAddress	Gets the high-level description of a configuration for StoreFront addresses, based on a configuration byte array.
Get-SfTask	Gets the task history for the Storefront Service.
New-SfCluster	Creates new Storefront cluster with default set of services.
New-SfStorefrontAddress	Creates a new StoreFront address configuration, specifying a single address.
Remove-SfServerFromCluster	Removes server from the cluster.
Remove-SfServiceMetadata	Removes metadata from the given Service.
Remove-SfTask	Removes from the database completed tasks for the Storefront Service.
Remove-SfTaskMetadata	Removes metadata from the given Task.
Reset-SfServiceGroupMembership	Reloads the access permissions and configuration service locations for the Storefront Service.
Set-SfCluster	Sets the parameters on the given cluster.
Set-SfDBConnection	Configures a database connection for the Storefront Service.
Set-SfServiceMetadata	Adds or updates metadata on the given Service.
Set-SfTaskMetadata	Adds or updates metadata on the given Task.
Test-SfDBConnection	Tests a database connection for the Storefront Service.

about_SfStorefrontSnapin

Sep 10, 2014

TOPIC

about_SfStorefrontSnapin

SHORT DESCRIPTION

This service short description

COMMAND PREFIX

All commands in this snap-in have the noun prefixed with 'Sf'.

LONG DESCRIPTION

This service long description

about_Sf_Filtering

Sep 10, 2014

TOPIC

XenDesktop - Advanced Dataset Filtering

SHORT DESCRIPTION

Describes the common filtering options for XenDesktop cmdlets.

LONG DESCRIPTION

Some cmdlets operate on large quantities of data and, to reduce the overhead of sending all of that data over the network, many of the Get- cmdlets support server-side filtering of the results.

The conventional way of filtering results in PowerShell is to pipeline them into Where-Object, Select-Object, and Sort-Object, for example:

```
Get-<Noun> | Where { $_.Size = 'Small' } | Sort 'Date' | Select -First 10
```

However, for most XenDesktop cmdlets the data is stored remotely and it would be slow and inefficient to retrieve large amounts of data over the network and then discard most of it. Instead, many of the Get- cmdlets provide filtering parameters that allow results to be processed on the server, returning only the required results.

You can filter results by most object properties using parameters derived from the property name. You can also sort results or limit them to a specified number of records:

```
Get-<Noun> -Size 'Small' -SortBy 'Date' -MaxRecordCount 10
```

You can express more complex filter conditions using a syntax and set of operators very similar to those used by PowerShell expressions.

Those cmdlets that support filtering have the following common parameters:

-MaxRecordCount <int>

Specifies the maximum number of results to return.
For example, to return only the first nine results use:

```
Get-<Noun> -MaxRecordCount 9
```

If not specified, only the first 250 records are returned, and if more are available, a warning is produced:

```
WARNING: Only first 250 records returned. Use -MaxRecordCount to
```

retrieve more.

You can suppress this warning by using -WarningAction or by specifying a value for -MaxRecordCount.

To retrieve all records, specify a large number for -MaxRecordCount. As the value is an integer, you can use the following:

```
Get-<Noun> -MaxRecordCount [int]::MaxValue
```

-ReturnTotalRecordCount [<SwitchParameter>]

When specified, this causes the cmdlet to output an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. For example:

```
Get-<Noun> -MaxRecordCount 9 -ReturnTotalRecordCount
....

Get-<Noun> : Returned 9 of 10 items
At line:1 char:18
+ Get-<Noun> <<<<  -MaxRecordCount 9 -ReturnTotalRecordCount
+ CategoryInfo          : OperationStopped: (:) [Get-<Noun>], PartialDataException
+ FullyQualifiedErrorId : PartialData,Citrix.<SDKName>.SDK.Get<Noun>
```

The count can be accessed using the TotalAvailableResultCount property:

```
$count = $error[0].TotalAvailableResultCount
```

-Skip <int>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

-SortBy <string>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order, respectively. Ascending order is assumed if no prefix is present.

Sorting occurs before -MaxRecordCount and -Skip parameters are
applied. For example, to sort by Name and then by Count (largest first)
use:

-SortBy 'Name,-Count'

By default, sorting by an enumeration property uses the numeric value
of the elements. You can specify a different sort order by qualifying
the name with an ordered list of elements or their numeric values,
or <null> to indicate the placement of null values.
Elements not mentioned are placed at the end in their numeric order.
For example, to sort by two different enums and then by the object id:

-SortBy 'MyState(StateC,<null>,StateA,StateB),Another(0,3,2,1),Id'

-Filter <String>

This parameter lets you specify advanced filter expressions, and
supports combination of conditions with -and and -or, and grouping
with braces. For example:

Get-<Noun> -Filter 'Name -like "High*" -or (Priority -eq 1 -and Severity -ge 2)'

The syntax is close enough to PowerShell syntax that you can use
script blocks in most cases. This can be easier to read as it reduces
quoting:

Get-<Noun> -Filter { Count -ne $null }

The full -Filter syntax is provided below.

EXAMPLES

Filtering by strings performs a case-insensitive wildcard match.
Separate parameters are combined with an implicit -and operator.
Normal PowerShell quoting rules apply, so you can use single or double
quotes, and omit the quotes altogether for many strings. The order of
parameters does not make any difference. The following are equivalent:

```
Get-<Noun> -Company Citrix -Product Xen*
Get-<Noun> -Company "citrix" -Product '[X]EN*'
Get-<Noun> -Product "Xen*" -Company "CITRIX"
Get-<Noun> -Filter { Company -eq 'Citrix' -and Product -like 'Xen*' }
```

See about_Quoting_Rules and about_Wildcards for details about PowerShell

handling of quotes and wildcards.

To avoid wildcard matching or include quote characters, you can escape the wildcards using the normal PowerShell escape mechanisms (see about_Escape_Characters), or switch to a filter expression and the -eq operator:

```
Get-<Noun> -Company "Abc[*]"              # Matches Abc*
Get-<Noun> -Company "Abc`*"               # Matches Abc*
Get-<Noun> -Filter { Company -eq "Abc*" }    # Matches Abc*
Get-<Noun> -Filter { Company -eq "A`"B`'C" } # Matches A"B'C
```

Simple filtering by numbers, booleans, and TimeSpans perform direct equality comparisons, although if the value is nullable you can also search for null values. Here are some examples:

```
Get-<Noun> -Uid 123
Get-<Noun> -Enabled $true
Get-<Noun> -Duration 1:30:40
Get-<Noun> -NullableProperty $null
```

More comparisons are possible using advanced filtering with -Filter:

```
Get-<Noun> -Filter 'Capacity -ge 10gb'
Get-<Noun> -Filter 'Age -ge 20 -and Age -lt 40'
Get-<Noun> -Filter 'VolumeLevel -like "[123]"'
Get-<Noun> -Filter 'Enabled -ne $false'
Get-<Noun> -Filter 'NullableProperty -ne $null'
```

You can check boolean values without an explicit comparison operator, and you can also combine them with -not:

```
Get-<Noun> -Filter 'Enabled'      # Equivalent to 'Enabled -eq $true'
Get-<Noun> -Filter '-not Enabled' # Equivalent to 'Enabled -eq $false'
```

See about_Comparison_Operators for an explanation of the operators, but note that only a subset of PowerShell operators are supported (-eq, -ne, -gt, -ge, -lt, -le, -like, -notlike, -in, -notin, -contains, -notcontains).

Enumeration values can either be specified using typed values or the string name of the enumeration value:

```
Get-<Noun> -Shape [Shapes]::Square
Get-<Noun> -Shape Circle
```

With filter expressions, typed values can be specified with simple variables or quoted strings. They also support enumerations with wildcards:

```
$s = [Shapes]::Square
Get-<Noun> -Filter { Shape -eq $s -or Shape -eq "Circle" }
Get-<Noun> -Filter { Shape -like 'C*' }
```

By their nature, floating point values, DateTime values, and TimeSpan values are best suited to relative comparisons rather than just equality. DateTime strings are converted using the locale and time zone of the user device, but you can use ISO8601 format strings (YYYY-MM-DDThh:mm:ss.sTZD) to avoid ambiguity. You can also use standard PowerShell syntax to create these values:

```
Get-<Noun> -Filter { StartTime -ge "2010-08-23T12:30:00.0Z" }
$d = [DateTime]"2010-08-23T12:30:00.0Z"
Get-<Noun> -Filter { StartTime -ge $d }
$d = (Get-Date).AddDays(-1)
Get-<Noun> -Filter { StartTime -ge $d }
```

Relative times are quite common and, when using filter expressions, you can also specify DateTime values using a relative format:

```
Get-<Noun> -Filter { StartTime -ge '-2' }        # Two days ago
Get-<Noun> -Filter { StartTime -ge '-1:30' }     # Hour and a half ago
Get-<Noun> -Filter { StartTime -ge '-0:0:30' }   # 30 seconds ago
```

ARRAY PROPERTIES

When filtering against list or array properties, simple parameters perform a case-insensitive wildcard match against each of the members. With filter expressions, you can use the -contains and -notcontains operators. Unlike PowerShell, these perform wildcard matching on strings.
Note that for array properties the naming convention is for the returned property to be plural, but the parameter used to search for any match is singular. The following are equivalent (assuming Users is an array property):

```
Get-<Noun> -User Fred*
Get-<Noun> -Filter { User -like "Fred*" }
Get-<Noun> -Filter { Users -contains "Fred*" }
```

You can also use the singular form with -Filter to search using other operators:

```
# Match if any user in the list is called "Frederick"
Get-<Noun> -Filter { User -eq "Frederick" }
# Match if any user in the list has a name alphabetically below 'F'
Get-<Noun> -Filter { User -lt 'F' }
```

COMPLEX EXPRESSIONS

When matching against multiple values, you can use a sequence of

comparisons joined with -or operators, or you can use -in and -notin:

```
Get-<Noun> -Filter { Shape -eq 'Circle' -or Shape -eq 'Square' }
$shapes = 'Circle','Square'
Get-<Noun> -Filter { Shape -in $shapes }
$sides = 1..4
Get-<Noun> -Filter { Sides -notin $sides }
```

Braces can be used to group complex expressions, and override the default left-to-right evaluation of -and and -or. You can also use -not to invert the sense of any sub-expression:

```
Get-<Noun> -Filter { Size -gt 4 -or (Color -eq 'Blue' -and Shape -eq 'Circle') }
Get-<Noun> -Filter { Sides -lt 5 -and -not (Color -eq 'Blue' -and Shape -eq 'Circle') }
```

PAGING

The simplest way to page through data is to use the -Skip and -MaxRecordCount parameters. So, to read the first three pages of data with 10 records per page, use:

```
Get-<Noun> -Skip 0  -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 10 -MaxRecordCount 10 <other filtering criteria>
Get-<Noun> -Skip 20 -MaxRecordCount 10 <other filtering criteria>
```

You must include the same filtering criteria on each call, and ensure that the data is sorted consistently.

The above approach is often acceptable, but as each call performs an independent query, data changes can result in records being skipped or appearing twice. One approach to improve this is to sort by a unique id field and then start the search for the next page at the unique id after the last unique id of the previous page. For example:

```
# Get the first page
Get-<Noun> -MaxRecordCount 10 -SortBy SerialNumber

SerialNumber  ...
------------  ---
A120004
A120007
... 7 other records ...
A120900

# Get the next page
Get-<Noun> -MaxRecordCount 10 -Filter { FirstName -gt 'A120900' }

SerialNumber  ...
------------  ---
```

A120901
B220000
...

FILTER SYNTAX DEFINITION

<Filter> ::= <ScriptBlock> | <ComponentList>

<ScriptBlock> ::= "{" <ComponentList> "}"

<ComponentList> ::= <Component> <AndOrOperator> <ComponentList> |

<Component>

<Component> ::= <NotOperator> <Factor> |

<Factor>

<Factor> ::= "(" <ComponentList> ")" |

<PropertyName> <ComparisonOperator> <Value> |
<PropertyName>

<AndOrOperator> ::= "-and" | "-or"

<NotOperator> ::= "-not" | "!"

<ComparisonOperator>

::= "-eq" | "-ne" | "-le" | "-ge" | "-lt" | "-gt" |
"-like" | "-notlike" | "-contains" | "-notcontains" |
"-in" | "-notin"

<PropertyName> ::= <simple name of property>

<Value> ::= <string literal> | <numeric literal> |

<scalar variable> | <array variable> |
"$null" | "$true" | "$false"

Numeric literals support decimal and hexadecimal literals, with optional multiplier suffixes (kb, mb, gb, tb, pb).

Dates and times can be specified as string literals. The current culture determines what formats are accepted. To avoid any ambiguity, use strings formatted to the ISO8601 standard. If not specified, the current time zone is used.

Relative date-time string literals are also supported, using a minus sign followed by a TimeSpan. For example, "-1:30" means 1 hour and 30 minutes ago.

Add-SfServerToCluster

Sep 10, 2014

Adds a new server to an existing cluster.

Syntax

```
Add-SfServerToCluster -ClusterId <Guid> -ServerName <String> [-StorefrontUrl <Uri>] [-FarmName <String>] [-XmlServices <Uri[]>] [-RunAsynchronously <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Adds a new server to an existing cluster. Optionally updates Farm and Storefront Url. After operation succeeds, all servers are configured identically.

Related topics

Get-SfCluster

New-SfCluster

Remove-SfServerFromCluster

Set-SfCluster

Parameters

-ClusterId<Guid>

The id of the cluster to perform operation on.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ServerName<String>

The name of the server to join to exisiting cluster. The name must be one of the values returned by Get-SfCluster

Required?	true
Default Value	
Accept Pipeline Input?	false

-StorefrontUrl<Uri>

The url that will be used by Receivers to contact Storefront. Http or https absolute urls are accepted.

Required?	false
Default Value	Server name and http binding.
Accept Pipeline Input?	false

-FarmName<String>

Name of the farm that will be used within Store service. Either both FarmName and XmlServices need to be specified or none of them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-XmlServices<Uri[]>

Collection of the url of xml services that will be used inside a farm. The urls neeed to be http or https, be absolute and share the same schema and port. Either both FarmName and XmlServices need to be specified or none of them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RunAsynchronously<Boolean>

If set, the command will run asynchronously.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Storefront.Sdk.Task or Citrix.Storefront.DataModel.Cluster

Returns cluster description or a task, if ran asynchronously.

Examples

---------- EXAMPLE 1 ----------

```
Add-SfServerToCluster -ClusterId (Guid) -ServerName NewSfServer -RunAsynchronously $true
```

Adds "NewSfServer" to cluster with id (Guid).

Add-SfStorefrontAddress

Sep 10, 2014

Modifies a StoreFront address configuration by adding an additional StoreFront address to it.

Syntax

```
Add-SfStorefrontAddress [-ByteArray] <Byte[]> -Name <String> -Url <String> -Enabled <Boolean> -Description <String> [<CommonParameters>]
```

Detailed Description

Use this command to transform an existing StoreFront configuration into a new configuration, where the new configuration contains one additional address. The original configuration is supplied as an input, along with the properties of the new StoreFront address being added. The cmdlet outputs the modified configuration, which can then be passed to the Citrix Broker Service using the Add-BrokerMachineConfiguration command.

This command does not, by itself, have any persistent effects within XenDesktop. To make the change persistent, the new configuration byte array must first be transformed into a machine configuration within the Citrix Broker Service. To do this, use the New-BrokerMachineConfiguration command. You can then use the Add-BrokerMachineConfiguration and Set-BrokerMachineConfiguration commands to fully associate the new configuration with a delivery group.

Related topics

New-SfStorefrontAddress

Get-SfStorefrontAddress

New-BrokerMachineConfiguration

Add-BrokerMachineConfiguration

Set-BrokerMachineConfiguration

Parameters

-ByteArray<Byte[]>

Specifies the initial configuration, on which the new configuration is based. All of the addresses in the original configuration are also present in the new configuration, along with the additional address specified. This configuration byte array is obtained from an earlier call to New-SfStorefrontAddress, or from Get-BrokerMachineConfiguration.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the name of the new StoreFront.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Url<String>

Specifies the URL to the StoreFront, such as "https://mysite.com/Citrix/StoreWeb".

Required?	true
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Specifies if the new StoreFront address should be enabled for user access.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Description<String>

Specifies a human-readable description of the new StoreFront.

Required?	true
Default Value	
Accept Pipeline Input?	false

Input Type

System.Byte[] This cmdlet accepts configurations as pipeline input, as an alternative to supplying the ByteArray parameter.

Return Values

System.Byte[]

This cmdlet outputs the new, modified configuration. This differs from the original configuration in that it contains the additional StoreFront address.

Examples

---------- EXAMPLE 1 ----------

C:\PS> $newConfiguration = Add-SfStorefrontAddress -ByteArray $originalConfiguration -Url "https://mysite.com/Citrix/StoreWeb" -Description "This StoreFront delivers my
This command transforms the configuration byte array specified by $originalConfiguration, adds the new StoreFront details, and stores the resulting configuration in $newConfiguration.

Get-SfCluster

Sep 10, 2014

Gets all Storefront clusters present in the site.

Syntax

```
Get-SfCluster [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Gets all Storefront clusters present in the site. There is one special Cluster with null id that lists the servers that are not part to any cluster (they are available to join any).

Related topics

New-SfCluster

Add-SfServerToCluster

Remove-SfServerFromCluster

Set-SfCluster

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Storefront.DataModel.Cluster[]

Returns array of clusters available in current deployment.

Get-SfDBConnection

Sep 10, 2014

Gets the database string for the specified data store used by the Storefront Service.

Syntax

```
Get-SfDBConnection [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the database connection string for the specified data store.

If the returned string is blank, no valid connection string has been specified. In this case the service is running, but is idle and awaiting specification of a valid connection string.

Related topics

Get-SfServiceStatus

Set-SfDBConnection

Test-SfDBConnection

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

system.string

The database connection string configured for the Storefront Service.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoDBConnections

The database connection string for the Storefront Service has not been specified.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-SfDBConnection

Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True
```

Get the database connection string for the Storefront Service.

Get-SfDBSchema

Sep 10, 2014

Gets a script that creates the Storefront Service database schema for the specified data store.

Syntax

Get-SfDBSchema [-DatabaseName <String>] [-ServiceGroupName <String>] [-ScriptType <ScriptTypes>] [-LocalDatabase] [-Sid <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Gets SQL scripts that can be used to create a new Storefront Service database schema, add a new Storefront Service to an existing site, remove a Storefront Service from a site, or create a database server logon for a Storefront Service. If no Sid parameter is provided, the scripts obtained relate to the currently selected Storefront Service instance, otherwise the scripts relate to Storefront Service instance running on the machine identified by the Sid provided. When obtaining the Evict script, a Sid parameter must be supplied. The current service instance is that on the local machine, or that explicitly specified by the last usage of the -AdminAddress parameter to a Storefront SDK cmdlet. The service instance used to obtain the scripts does not need to be a member of a site or to have had its database connection configured. The database scripts support only Microsoft SQL Server, or SQL Server Express, and require Windows integrated authentication to be used. They can be run using SQL Server's SQLCMD utility, or by copying the script into an SQL Server Management Studio (SSMS) query window and executing the query. If using SSMS, the query must be executed in 'SMDCMD mode'. The ScriptType parameter determines which script is obtained. If ScriptType is not specified, or is FullDatabase, the script contains:

o Creation of service schema

o Creation of database server logon

o Creation of database user

o Addition of database user to Storefront Service roles

If ScriptType is Instance, the returned script contains:

o Creation of database server logon

o Creation of database user

o Addition of database user to Storefront Service roles

If ScriptType is Evict, the returned script contains:

o Removal of Storefront Service instance from database

o Removal of database user

If ScriptType is Login, the returned script contains:

o Creation of database server logon only

If the service uses two data stores they can exist in the same database. You do not need to configure a database before using this command.

Related topics

Set-SfDBConnection

Parameters

-DatabaseName<String>

Specifies the name of the database for which the schema will be generated.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ServiceGroupName<String>

Specifies the name of the service group to be used when creating the database schema. The service group is a collection of all the Storefront services that share the same database instance and are considered equivalent; that is, all the services within a service group can be used interchangeably.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ScriptType<ScriptTypes>

Specifies the type of database script returned. Available script types are:

Database

Returns a full database script that can be used to create a database schema for the Storefront Service in a database instance that does not already contain a schema for this service. The DatabaseName and ServiceGroupName parameters must be specified to create a script of this type.

Instance

Returns a permissions script that can be used to add further Storefront services to an existing database instance that already contains the full Storefront service schema, associating the services to the Service Group. The Sid parameter can optionally be specified to create a script of this type.

Login

Returns a database logon script that can be used to add the required logon accounts to an existing database instance that contains the Storefront Service schema. This is used primarily when creating a mirrored database environment. The

DatabaseName parameter must be specified to create a script of this type.

Evict

Returns a script that can be used to remove the specified Storefront Service from the database entirely. The DatabaseName and Sid parameters must be specified to create a script of this type.

Required?	false
Default Value	Database
Accept Pipeline Input?	false

-LocalDatabase<SwitchParameter>

Specifies whether the database script is to be used in a database instance run on the same controller as other services in the service group. Including this parameter ensures the script creates only the required permissions for local services to access the database schema for Storefront services.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Sid<String>

Specifies the SID of the controller on which the Storefront Service instance to remove from the database is running.

Required?	false
Default Value	
Accept Pipeline Input?	true (ByValue)

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.string

A string containing the required SQL script for application to a database.

Notes

The scripts returned support Microsoft SQL Server Express Edition, Microsoft SQL Server Standard Edition, and Microsoft SQL Server Enterprise Edition databases only, and are generated on the assumption that integrated authentication will be used.

If the ScriptType parameter is not included or set to 'FullDatabase', the full database script is returned, which will:

Create the database schema.

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist).

If the ScriptType parameter is set to 'Instance', the script will:

Create the user and the role (providing the schema does not already exist).

Create the logon (providing the schema does not already exist) and associate it with a user.

If the ScriptType parameter is set to 'Login', the script will:

Create the logon (providing the schema does not already exist) and associate it with a pre-existing user of the same name.

If the LocalDatabase parameter is included, the NetworkService account will be added to the list of accounts permitted to access the database. This is required only if the database is run on a controller.

If the command fails, the following errors can be returned.

Error Codes

GetSchemasFailed

The database schema could not be found.

ActiveDirectoryAccountResolutionFailed

The specified Active Directory account or Group could not be found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-SfDBSchema -DatabaseName MyDB -ServiceGroupName  MyServiceGroup > c:\SfSchema.sql
```

Get the full database schema for site data store of the Storefront Service and copy it to a file called 'c:\SfSchema.sql'.

This script can then be used to create the schema in a pre-existing database named 'MyDB' that does not already contain a Storefront Service site schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-SfDBSchema -DatabaseName MyDB -scriptType Login > c:\StorefrontLogins.sql
```

Get the logon scripts for the Storefront Service.

Get-SfDBVersionChangeScript

Sep 10, 2014

Gets a script that updates the Storefront Service database schema.

Syntax

```
Get-SfDBVersionChangeScript -DatabaseName <String> -TargetVersion <Version> [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns a database script that can be used to upgrade or downgrade the site or secondary schema for the Storefront Service from the current schema version to a different version.

Related topics

Get-SfInstalledDBVersion

Parameters

-DatabaseName<String>

Specifies the name of the database instance to which the update applies.

Required?	true
Default Value	
Accept Pipeline Input?	false

-TargetVersion<Version>

Specifies the version of the database you want to update to.

Required?	true
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Management.Automation.PSObject

A PSObject containing the required SQL script for application to a database.

Notes

The PSObject returned by this cmdlet contains the following properties:

-- Script The raw text of the SQL script to apply the update, or null in the case when no upgrade path to the specified target version exists.

-- NeedExclusiveAccess Indicates whether all services in the service group must be shut down during the update or not.

-- CanUndo Indicates whether the generated script allows the updated schema to be reverted to the state prior to the update.

Scripts to update the schema version are stored in the database so any service in the service group can obtain these scripts. Extreme caution should be exercised when using update scripts. Citrix recommends backing up the database before attempting to upgrade the schema. Database update scripts may require exclusive use of the schema and so may not be able to execute while any Storefront services are running. However, this depends on the specific update being carried out.

After a schema update has been carried out, services that require the previous version of the schema may cease to operate. The ServiceState parameter reported by the Get-SfServiceStatus command provides information about service compatibility. For example, if the schema has been upgraded to a more recent version that a service cannot use, the service reports "DBNewerVersionThanService".

If the command fails, the following errors can be returned.

Error Codes

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Storefront Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
C:\PS> $update = Get-SfDBVersionChangeScript -DatabaseName MyDb -TargetVersion 1.0.75.0
C:\PS> $update.Script > update_75.sql
```

Gets an SQL update script to update the current schema to version 1.0.75.0. The resulting update_75.sql script is suitable for direct use with the SQL Server SQLCMD utility.

Get-SfInstalledDBVersion

Sep 10, 2014

Gets a list of all available database schema versions for the Storefront Service.

Syntax

```
Get-SfInstalledDBVersion [-Upgrade] [-Downgrade] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns the current version of the Storefront Service database schema, if no flags are set, otherwise returns versions for which upgrade or downgrade scripts are available and have been stored in the database.

Related topics

Parameters

-Upgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be updated should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-Downgrade<SwitchParameter>

Specifies that only schema versions to which the current database version can be reverted should be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.

Accept Pipeline Input?	false

Return Values

System.Version

The Get-SfInstalledDbVersion command returns objects containing the new definition of the Storefront Service database schema version.

Major <Integer>

Minor <Integer>

Build <Integer>

Revision <Integer>

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

Both the Upgrade and Downgrade flags were specified.

NoOp

The operation was successful but had no effect.

NoDBConnections

The database connection string for the Storefront Service has not been specified.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-SfInstalledDBVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      6      0      0
```

Get the currently installed version of the Storefront Service database schema.

---------- EXAMPLE 2 ----------

```
c:\PS>Get-SfInstalledDBVersion -Upgrade

Major  Minor  Build  Revision
-----  -----  -----  --------
6      0      0      0
```

Get the versions of the Storefront Service database schema for which upgrade scripts are supplied.

Get-SfIsStorefrontInstalled

Sep 10, 2014

Tells whether StoreFront Services and Privileged Service are installed.

Syntax

```
Get-SfIsStorefrontInstalled [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

bool

True if both StoreFront Services and Privileged Service are installed, false otherwise.

Get-SfService

Sep 10, 2014

Gets the service record entries for the Storefront Service.

Syntax

Get-SfService [-Metadata <String>] [-Property <String[]>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns instances of the Storefront Service that the service publishes. The service records contain account security identifier information that can be used to remove each service from the database.

A database connection for the service is required to use this command.

Related topics

Parameters

-Metadata<String>

Gets records with matching metadata entries.

The value being compared with is a concatenation of the key name, a colon, and the value. For example: -Metadata "abc:x*" matches records with a metadata entry having a key name of "abc" and a value starting with the letter "x".

Required?	false
Default Value	
Accept Pipeline Input?	false

-Property<String[]>

Specifies the properties to be be returned. This is similar to piping the output of the command through Select-Object, but the properties are filtered more efficiently at the server.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Sf_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.

Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Sf_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Storefront.Sdk.Service

The Get-SfServiceInstance command returns an object containing the following properties.

Uid <Integer>

Specifies the unique identifier for the service in the group. The unique identifier is an index number.

ServiceHostId <Guid>

Specifies the unique identifier for the service instance.

DNSName <String>

Specifies the domain name of the host on which the service runs.

MachineName <String>

Specifies the short name of the host on which the service runs.

CurrentState <Citrix.Fma.Sdk.ServiceCore.ServiceState>

Specifies whether the service is running, started but inactive, stopped, or failed.

LastStartTime <DateTime>

Specifies the date and time at which the service was last restarted.

LastActivityTime <DateTime>

Specifies the date and time at which the service was last stopped or restarted.

OSType

Specifies the operating system installed on the host on which the service runs.

OSVersion

Specifies the version of the operating system installed on the host on which the service runs.

ServiceVersion

Specifies the version number of the service instance. The version number is a string that reflects the full build version of the service.

DatabaseUserName <string>

Specifies for the service instance the Active Directory account name with permissions to access the database. This will be either the machine account or, if the database is running on a controller, the NetworkService account.

Sid <string>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

ActiveSiteServices <string[]>

Specifies the names of active site services currently running in the service. Site services are components that perform long-running background processing in some services. This field is empty for services that do not contain site services.

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-SfService

Uid             : 1
ServiceHostId     : aef6f464-f1ee-4042-a523-66982e0cecd0
DNSName           : MyServer.company.com
MachineName       : MYSERVER
CurrentState      : On
LastStartTime     : 04/04/2011 15:25:38
LastActivityTime  : 04/04/2011 15:33:39
OSType            : Win32NT
OSVersion         : 6.1.7600.0
ServiceVersion    : 5.1.0.0
DatabaseUserName  : NT AUTHORITY\NETWORK SERVICE
SID               : S-1-5-21-2316621082-1546847349-2782505528-1165
ActiveSiteServices : {MySiteService1, MySiteService2...}
```

Get all the instances of the Storefront Service running in the current service group.

Get-SfServiceAddedCapability

Sep 10, 2014

Gets any added capabilities for the Storefront Service on the controller.

Syntax

```
Get-SfServiceAddedCapability [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables updates to the Storefront Service on the controller to be detected.

You do not need to configure a database connection before using this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.String

String containing added capabilities.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-SfServiceAddedCapability
```

Get the added capabilities of the Storefront Service.

Get-SfServiceInstance

Sep 10, 2014

Gets the service instance entries for the Storefront Service.

Syntax

```
Get-SfServiceInstance [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Returns service interfaces published by the instance of the Storefront Service. Each instance of a service publishes multiple interfaces with distinct interface types, and each of these interfaces is represented as a ServiceInstance object. Service instances can be used to register the service with a central configuration service so that other services can use the functionality.

You do not need to configure a database connection to use this command.

Related topics

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Storefront.Sdk.ServiceInstance

The Get-SfServiceInstance command returns an object containing the following properties.

ServiceGroupUid <Guid>

Specifies the unique identifier for the service group of which the service is a member.

ServiceGroupName <String>

Specifies the name of the service group of which the service is a member.

ServiceInstanceUID <Guid>

Specifies the unique identifier for registered service instances, which are service instances held by and obtained from a

central configuration service. Unregistered service instances do not have unique identifiers.

ServiceType <String>

Specifies the service instance type. For this service, the service instance type is always Sf.

Address

Specifies the address of the service instance. The address can be used to access the service and, when registered in the central configuration service, can be used by other services to access the service.

Binding

Specifies the binding type that must be used to communicate with the service instance. In this release of XenDesktop, the binding type is always 'wcf_HTTP_kerb'. This indicates that the service provides a Windows Communication Foundation endpoint that uses HTTP binding with integrated authentication.

Version

Specifies the version of the service instance. The version number is used to ensure that the correct versions of the services are used for communications.

ServiceAccount <String>

Specifies the Active Directory account name for the machine on which the service instance is running. The account name is used to provide information about the permissions required for interservice communications.

ServiceAccountSid <String>

Specifies the Active Directory account security identifier for the machine on which the service instance is running.

InterfaceType <String>

Specifies the interface type. Each service can provide multiple service instances, each for a different purpose, and the interface defines the purpose. Available interfaces are:

SDK - for PowerShell operations

InterService - for operations between different services

Peer - for communications between services of the same type

Metadata <Citrix.Storefront.Sdk.Metadata[]>

The collection of metadata associated with registered service instances, which are service instances held by and obtained from a central configuration service. Metadata is not stored for unregistered service instances.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-SfServiceInstance

Address          : http://MyServer.com:80/Citrix/StorefrontContract
Binding          : wcf_HTTP_kerb
InterfaceType    : SDK
Metadata         :
MetadataMap      :
ServiceAccount   : ENG\MyAccount$
ServiceAccountSid : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName  : MyServiceGroup
ServiceGroupUid   : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType      : Sf
Version          : 1

Address          : http://MyServer.com:80/Citrix/StorefrontContract/IServiceApi
Binding          : wcf_HTTP_kerb
InterfaceType    : InterService
Metadata         :
MetadataMap      :
```



```
ServiceAccount     : ENG\MyAccount
ServiceAccountSid  : S-1-5-21-2406005612-3133289213-1653143164
ServiceGroupName   : MyServiceGroup
ServiceGroupUid    : a88d2f6b-c00a-4f76-9c38-e8330093b54d
ServiceInstanceUid : 00000000-0000-0000-0000-000000000000
ServiceType        : Sf
Version            : 1
```

Get all instances of the Storefront Service running on the specified machine. For remote services, use the AdminAddress parameter to define the service for which the interfaces are required. If the AdminAddress parameter has not been specified for the runspace, service instances running on the local machine are returned.

Get-SfServiceStatus

Sep 10, 2014

Gets the current status of the Storefront Service on the controller.

Syntax

```
Get-SfServiceStatus [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables the status of the Storefront Service on the controller to be monitored. If the service has multiple data stores it will return the overall state as an aggregate of all the data store states. For example, if the site data store status is OK and the secondary data store status is DBUnconfigured then it will return DBUnconfigured.

Related topics

Set-SfDBConnection

Test-SfDBConnection

Get-SfDBConnection

Get-SfDBSchema

Parameters

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Get-SfServiceStatus command returns an object containing the status of the Storefront Service together with extra diagnostics information.

DBUnconfigured

The Storefront Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the Storefront Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Storefront Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Storefront Service currently in use is incompatible with the version of the Storefront Service schema on the database. Upgrade the Storefront Service to a more recent version.

DBOlderVersionThanService

The version of the Storefront Service schema on the database is incompatible with the version of the Storefront Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Storefront Service is running and is connected to a database containing a valid schema.

Failed

The Storefront Service has failed.

Unknown

(0) The service status cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-SfServiceStatus

DBUnconfigured
```

Get the current status of the Storefront Service.

Get-SfStorefrontAddress

Sep 10, 2014

Gets the high-level description of a configuration for StoreFront addresses, based on a configuration byte array.

Syntax

```
Get-SfStorefrontAddress [-ByteArray] <Byte[]> [<CommonParameters>]
```

Detailed Description

Use this command to convert a configuration byte array into a set of named property settings. The byte array will either have been retrieved from the Citrix Broker Service, or from the New-SfStorefrontAddress cmdlet.

Related topics

New-SfStorefrontAddress

Add-SfStorefrontAddress

New-BrokerMachineConfiguration

Add-BrokerMachineConfiguration

Set-BrokerMachineConfiguration

Parameters

-ByteArray<Byte[]>

Specifies the low-level byte array (blob) to be interpreted.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

Input Type

System.Byte[] The cmdlet accepts the ByteArray parameter as pipeline input.

Return Values

Citrix.Storefront.Sdk.SfStorefrontAddress

This cmdlet outputs one SfStorefrontAddress object for each address that is configured within the slot. Each object has the following properties:

Name - Specifies the name of the StoreFront.

Url - Specifies the URL to the StoreFront, such as "https://mysite.com/Citrix/StoreWeb".

Enabled - Specifies whether the StoreFront is enabled for users.

Description - Specifies the human-readable name of the StoreFront.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $configuration = New-SfStorefrontAddress -Url "https://mysite.com/Citrix/StoreWeb" -Description "This StoreFront delivers my corporate applications" -Name "Store

C:\PS> Get-SfStorefrontAddress -ByteArray $configuration

Name          Url                          Enabled Description
----          ---                          ------- -----------
StoreFront1   https://mysite.com/Citrix/StoreWeb   True This StoreFront delivers my corporate applications.
```

This example shows a new configuration byte array being created to specify a single StoreFront address. The configuration byte array is then provided as input to the Get-SfStorefrontAddress command, which interprets and outputs the same fields.

Get-SfTask

Sep 10, 2014

Gets the task history for the Storefront Service.

Syntax

Get-SfTask [[-TaskId] <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Returns a list of tasks that have run or are currently running within the Storefront Service.

Related topics

Remove-SfTask

Add-SfTaskMetadata

Remove-SfTaskMetadata

Parameters

-TaskId<Guid>

Specifies the task identifier to be returned.

Required?	false
Default Value	
Accept Pipeline Input?	false

-ReturnTotalRecordCount<SwitchParameter>

When specified, the cmdlet outputs an error record containing the number of records available. This error record is additional information and does not affect the objects written to the output pipeline. See about_Sf_Filtering for details.

Required?	false
Default Value	False
Accept Pipeline Input?	false

-MaxRecordCount<Int32>

Specifies the maximum number of records to return.

Required?	false
Default Value	250
Accept Pipeline Input?	false

-Skip<Int32>

Skips the specified number of records before returning results. Also reduces the count returned by -ReturnTotalRecordCount.

Required?	false
Default Value	0
Accept Pipeline Input?	false

-SortBy<String>

Sorts the results by the specified list of properties. The list is a set of property names separated by commas, semi-colons, or spaces. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Required?	false
Default Value	The default sort order is by name or unique identifier.
Accept Pipeline Input?	false

-Filter<String>

Gets records that match a PowerShell-style filter expression. See about_Sf_Filtering for details.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

UnknownObject

One of the specified objects was not found.

PartialData

Only a subset of the available data was returned.

InvalidFilter

A filtering expression was supplied that could not be interpreted for this cmdlet.

CouldNotQueryDatabase

The query required to get the database was not defined.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration service.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

New-SfCluster

Sep 10, 2014

Creates new Storefront cluster with default set of services.

Syntax

New-SfCluster -ServerName <String> -FarmName <String> -XmlServices <Uri[]> [-StorefrontUrl <Uri>] [-RunAsynchronously <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

The server will have a default set of services containing fully-functionaly Storefront server with Authentication, Store, Receiver for Web and Desktop Appliance.

Related topics

Get-SfCluster

Add-SfServerToCluster

Remove-SfServerFromCluster

Set-SfCluster

Parameters

-ServerName<String>

The name of the server to build a cluster on. The name must be one of the values returned by Get-SfCluster

Required?	true
Default Value	
Accept Pipeline Input?	false

-FarmName<String>

Name of the farm that will be used within Store service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-XmlServices<Uri[]>

Collection of the url of xml services that will be used inside a farm. The urls neeed to be http or https, be absolute and share the same schema and port.

Required?	true
Default Value	

Accept Pipeline Input?	false

-StorefrontUrl<Uri>

The url that will be used by Receivers to contact Storefront. Http or https absolute urls are accepted.

Required?	false
Default Value	Server name and http binding.
Accept Pipeline Input?	false

-RunAsynchronously<Boolean>

If set, the command will run asynchronously.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Storefront.Sdk.Task or Citrix.Storefront.DataModel.Cluster

Returns cluster description or a task, if ran asynchronously.

Examples

---------- EXAMPLE 1 ----------

```
New-SfCluster -FarmName "XdSiteName" -XmlServices http://farm1,http://farm2 -ServerName SfServer -RunAsynchronously $true
```

Creates a new cluster on server "SfServer". The server will have a default set of services containing fully-functionaly Storefront server with Authentication, Store, Receiver for Web, Desktop Appliance site and the required infrastructure. The Store service will have a farm named "XdSiteName" that will contain servers farm1 and farm2, whose will be contacted using http on default port 80.

New-SfStorefrontAddress

Sep 10, 2014

Creates a new StoreFront address configuration, specifying a single address.

Syntax

```
New-SfStorefrontAddress -Name <String> -Url <String> -Enabled <Boolean> -Description <String> [<CommonParameters>]
```

Detailed Description

Use this command when you want to create a new StoreFront configuration byte array from scratch, rather than modifying an existing one. You must define the URL for the StoreFront, and some additional details.

This command does not, by itself, have any persistent effects within XenDesktop. To make the change persistent, the new configuration byte array must first be transformed into a machine configuration within the Citrix Broker Service. To do this, use the New-BrokerMachineConfiguration command. You can then use the Add-BrokerMachineConfiguration and Set-BrokerMachineConfiguration commands to fully associate the new configuration with a delivery group.

Related topics

Add-SfStorefrontAddress

Get-SfStorefrontAddress

New-BrokerMachineConfiguration

Add-BrokerMachineConfiguration

Set-BrokerMachineConfiguration

Parameters

-Name<String>

Specifies the name of the new StoreFront.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Url<String>

Specifies the URL to the StoreFront, such as "https://mysite.com/Citrix/StoreWeb".

Required?	true
Default Value	
Accept Pipeline Input?	false

-Enabled<Boolean>

Specifies if the new StoreFront address should be enabled for user access.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Description<String>

Specifies a human-readable description of the new StoreFront.

Required?	true
Default Value	
Accept Pipeline Input?	false

Input Type

None

Return Values

System.Byte[]

The new configuration set, with all of the given modifications applied.

Examples

---------- EXAMPLE 1 ----------

```
C:\PS> $configuration = New-SfStorefrontAddress -Url "https://mysite.com/Citrix/StoreWeb" -Description "This StoreFront delivers my corporate applications" -Name "Store

C:\PS> Get-SfStorefrontAddress -ByteArray $configuration

Name             Url                          Enabled Description
----             ---                          ------- -----------
StoreFront1      https://mysite.com/Citrix/StoreWeb       True This StoreFront delivers my corporate applications.
```

This example shows a new configuration byte array being created to specify a single StoreFront address. The configuration byte array is then provided as input to the Get-SfStorefrontAddress command, which interprets and outputs the same fields.

Remove-SfServerFromCluster

Sep 10, 2014

Removes server from the cluster.

Syntax

Remove-SfServerFromCluster -ClusterId <Guid> -ServerName <String> [-StorefrontUrl <Uri>] [-FarmName <String>] [-XmlServices <Uri[]>] [-RunAsynchronously <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Removes server from the cluster and propagates information to other servers. The configuration of the server is wiped out, so the server can be reused.

Related topics

Get-SfCluster

New-SfCluster

Add-SfServerToCluster

Set-SfCluster

Parameters

-ClusterId<Guid>

The if of the cluster to perform operation on.

Required?	true
Default Value	
Accept Pipeline Input?	false

-ServerName<String>

The name of the server to remove from cluster. The name must be one of the values returned by Get-SfCluster.

Required?	true
Default Value	
Accept Pipeline Input?	false

-StorefrontUrl<Uri>

The url that will be used by Receivers to contact Storefront. Http or https absolute urls are accepted.

Required?	false
Default Value	Server name and http binding.
Accept Pipeline Input?	false

-FarmName<String>

Name of the farm that will be used within Store service. Either both FarmName and XmlServices need to be specified or none of them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-XmlServices<Uri[]>

Collection of the url of xml services that will be used inside a farm. The urls neeed to be http or https, be absolute and share the same schema and port. Either both FarmName and XmlServices need to be specified or none of them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RunAsynchronously<Boolean>

If set, the command will run asynchronously.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Storefront.Sdk.Task or Citrix.Storefront.DataModel.Cluster

Returns cluster description or a task, if ran asynchronously.

Examples

---------- EXAMPLE 1 ----------

```
Remove-SfServerFromCluster -ClusterId (Guid) -ServerName BrokenSfServer -RunAsynchronously $true
```

Removes Server "BrokenSfServer" from a Cluster with id (Guid).

Remove-SfServiceMetadata

Sep 10, 2014

Removes metadata from the given Service.

Syntax

```
Remove-SfServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-SfServiceMetadata [-ServiceHostId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-SfServiceMetadata [-InputObject] <Service[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-SfServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Service.

Related topics

Set-SfServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-SfService | % { Remove-SfServiceMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Service objects.

Remove-SfTask

Sep 10, 2014

Removes from the database completed tasks for the Storefront Service.

Syntax

```
Remove-SfTask [-TaskId] <Guid> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Enables completed tasks that have run within the Storefront Service to be removed from the database.

Related topics

Get-SfTask

Add-SfTaskMetadata

Remove-SfTaskMetadata

Parameters

-TaskId<Guid>

Specifies the identifier for the task to be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByPropertyName)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

System.Management.Automation.PSObject Objects containing the TaskId parameter can be piped to the Remove-SfTask command.

Notes

If the command fails, the following errors can be returned.

Error Codes

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

ServiceStatusInvalidDb

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration service.

OperationDeniedByConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Remove-SfTaskMetadata

Sep 10, 2014

Removes metadata from the given Task.

Syntax

```
Remove-SfTaskMetadata [-TaskId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-SfTaskMetadata [-TaskId] <Guid> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-SfTaskMetadata [-InputObject] <Task[]> -Name <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Remove-SfTaskMetadata [-InputObject] <Task[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability to remove metadata from the given Task.

Related topics

Set-SfTaskMetadata

Parameters

-TaskId<Guid>

Id of the Task

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Task[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can be either a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]"). The properties whose names match keys in the map will be removed.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

The metadata property to remove.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Get-SfTask | % { Remove-SfTaskMetadata -Map $_.MetadataMap }
```

Remove all metadata from all Task objects.

Reset-SfServiceGroupMembership

Sep 10, 2014

Reloads the access permissions and configuration service locations for the Storefront Service.

Syntax

```
Reset-SfServiceGroupMembership [-ConfigServiceInstance] <ServiceInstance[]> [-LoggingId <Guid>] [-AdminAddress <String>]
[<CommonParameters>]
```

Detailed Description

Enables you to reload Storefront Service access permissions and configuration service locations. The Reset-SfServiceGroupMembership command must be run on at least one instance of the service type (Sf) after installation and registration with the configuration service. Without this operation, the Storefront services will be unable to communicate with other services in the XenDesktop deployment. When the command is run, the services are updated when additional services are added to the deployment, provided that the configuration service is not stopped. The Reset-SfServiceGroupMembership command can be run again to refresh this information if automatic updates do not occur when new services are added to the deployment. If more than one configuration service instance is passed to the command, the first instance that meets the expected service type requirements is used.

Related topics

Parameters

-ConfigServiceInstance<ServiceInstance[]>

Specifies the configuration service instance object that represents the service instance for the type 'InterService' that references a configuration service for the deployment.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Input Type

Citrix.Storefront.Sdk.ServiceInstance[] Service instances containing a ServiceInstance object that refers to the central configuration service interservice interface can be piped to the Reset-SfServiceGroupMembership command.

Notes

If the command fails, the following errors can be returned.

Error Codes

NoSuitableServiceInstance

None of the supplied service instance objects were suitable for resetting service group membership.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-SfServiceGroupMembership
```

Reset the service group membership for a service in a deployment where the configuration service is configured and running on the same machine as the service.

-------------------------- EXAMPLE 2 --------------------------

```
c:\PS>Get-ConfigRegisterdServiceInstance -ServiceType Config -AdminAddress OtherServer.example.com | Reset-SfServiceGroupmembership
```

Reset the service group membership for a service in a deployment where the configuration service that is configured and running on a machine named 'OtherServer.example.com'.

Set-SfCluster

Sep 10, 2014

Sets the parameters on the given cluster.

Syntax

```
Set-SfCluster -ClusterId <Guid> [-StorefrontUrl <Uri>] [-FarmName <String>] [-XmlServices <Uri[]>] [-RunAsynchronously <Boolean>] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Sets the parameters on the given cluster and propagate the changes to all servers within a given cluster.

Related topics

Get-SfCluster

New-SfCluster

Add-SfServerToCluster

Remove-SfServerFromCluster

Parameters

-ClusterId<Guid>

The if of the cluster to perform operation on.

Required?	true
Default Value	
Accept Pipeline Input?	false

-StorefrontUrl<Uri>

The url that will be used by Receivers to contact Storefront. Http or https absolute urls are accepted.

Required?	false
Default Value	Server name and http binding.
Accept Pipeline Input?	false

-FarmName<String>

Name of the farm that will be used within Store service. Either both FarmName and XmlServices need to be specified or none of them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-XmlServices<Uri[]>

Collection of the url of xml services that will be used inside a farm. The urls neeed to be http or https, be absolute and share the same schema and port. Either both FarmName and XmlServices need to be specified or none of them.

Required?	false
Default Value	
Accept Pipeline Input?	false

-RunAsynchronously<Boolean>

If set, the command will run asynchronously.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Storefront.Sdk.Task or Citrix.Storefront.DataModel.Cluster

Returns cluster description or a task, if ran asynchronously.

Examples

---------- EXAMPLE 1 ----------

```
Set-SfCluster -StorefrontUrl http://SfUrl -ClusterId (Guid) -RunAsynchronously $true
```

Sets a Storefront Url in a Cluster with id (Guid). Propagates changes to all servers that are part of the cluster.

Set-SfDBConnection

Sep 10, 2014

Configures a database connection for the Storefront Service.

Syntax

```
Set-SfDBConnection [-DBConnection] <String> [-Force] [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Configures a connection to a database in which the Storefront Service can store its state. The service will attempt to connect and start using the database immediately after the connection is configured. The database connection string is updated to the specified value regardless of whether it is valid or not. Specifying an invalid connection string prevents a service from functioning until the error is corrected.

After a connection is configured, you cannot alter it without first clearing it (by setting the connection to $null).

You do not need to configure a database connection to use this command.

Related topics

Get-SfServiceStatus

Get-SfDBConnection

Test-SfDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be used by the Storefront Service. Passing in $null will clear any existing database connection configured.

Required?	true
Default Value	
Accept Pipeline Input?	false

-Force<SwitchParameter>

If present, allows the local administrator to set the connection string to null when there are problems contacting the database or other services.

Required?	false
Default Value	false
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Set-SfDBConnection command returns an object containing the status of the Storefront Service together with extra diagnostics information.

DBUnconfigured

The Storefront Service does not have a database connection configured.

DBRejectedConnection

The database rejected the logon attempt from the Storefront Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Storefront Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Storefront Service currently in use is incompatible with the version of the Storefront Service schema on the database. Upgrade the Storefront Service to a more recent version.

DBOlderVersionThanService

The version of the Storefront Service schema on the database is incompatible with the version of the Storefront Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Storefront Service is running and is connected to a database containing a valid schema.

Failed

The Storefront Service has failed.

Unknown

The status of the Storefront Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

DatabaseConnectionDetailsAlreadyConfigured

There was already a database connection configured. After a configuration is set, it can only be set to $null.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-SfDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName;  Integrated Security = True"

OK
```

Configures a database connection string for the Storefront Service.

---------- EXAMPLE 2 ----------

```
c:\PS>Set-SfDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
```

Configures an invalid database connection string for the Storefront Service.

Set-SfServiceMetadata

Sep 10, 2014

Adds or updates metadata on the given Service.

Syntax

Set-SfServiceMetadata [-ServiceHostId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-SfServiceMetadata [-ServiceHostId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-SfServiceMetadata [-InputObject] <Service[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-SfServiceMetadata [-InputObject] <Service[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Detailed Description

Allows you to store additional custom data against given Service objects.

Related topics

Remove-SfServiceMetadata

Parameters

-ServiceHostId<Guid>

Id of the Service

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Service[]>

Objects to which metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Service specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false

Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-SfServiceMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

---------- EXAMPLE 1 ----------

```
c:\PS>Set-SfServiceMetadata -ServiceHostId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                             Value
        ---                             -----
        property                            value
```

Add metadata with a name of 'property' and a value of 'value' to the Service with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Set-SfTaskMetadata

Sep 10, 2014

Adds or updates metadata on the given Task.

Syntax

```
Set-SfTaskMetadata [-TaskId] <Guid> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-SfTaskMetadata [-TaskId] <Guid> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-SfTaskMetadata [-InputObject] <Task[]> -Map <PSObject> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]

Set-SfTaskMetadata [-InputObject] <Task[]> -Name <String> -Value <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Provides the ability for additional custom data to be stored against given Task objects.

Related topics

Remove-SfTaskMetadata

Parameters

-TaskId<Guid>

Id of the Task

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue, ByPropertyName)

-InputObject<Task[]>

Objects to which the metadata is to be added.

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Map<PSObject>

Specifies a dictionary of (name, value)-pairs for the properties. This can either be a hashtable (created with @{"name1" = "val1"; "name2" = "val2"}) or a string dictionary (created with new-object "System.Collections.Generic.Dictionary[String,String]").

Required?	true
Default Value	
Accept Pipeline Input?	true (ByValue)

-Name<String>

Specifies the property name of the metadata to be added. The property must be unique for the Task specified. The property cannot contain any of the following characters \/;:#.*?=<>|[]()"'

Required?	true
Default Value	
Accept Pipeline Input?	false

-Value<String>

Specifies the value for the property.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

System.Collections.Generic.Dictionary[String,String]

Set-SfTaskMetadata returns a dictionary containing the new (name, value)-pairs.

Key <string>

Specifies the name of the property.

Value <string>

Specifies the value for the property.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidParameterCombination

The cmdlet parameters are inconsistent.

UnknownObject

One of the specified objects was not found.

DatabaseError

An error occurred in the service while attempting a database operation.

DatabaseNotConfigured

The operation could not be completed because the database for the service is not configured.

DataStoreException

An error occurred in the service while attempting a database operation - communication with the database failed for various

reasons.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

```
c:\PS>Set-SfTaskMetadata -TaskId 4CECC26E-48E1-423F-A1F0-2A06DDD0805C -Name property -Value value

        Key                           Value
        ---                           -----
        property                          value
```

Add metadata with a name of 'property' and a value of 'value' to the Task with the identifier '4CECC26E-48E1-423F-A1F0-2A06DDD0805C'.

Test-SfDBConnection

Sep 10, 2014

Tests a database connection for the Storefront Service.

Syntax

```
Test-SfDBConnection [-DBConnection] <String> [-LoggingId <Guid>] [-AdminAddress <String>] [<CommonParameters>]
```

Detailed Description

Tests a connection to the database in which the Storefront Service can store its state. The service will attempt to connect to the database without affecting the current connection to the database.

You do not have to clear the connection to use this command.

Related topics

Get-SfServiceStatus

Get-SfDBConnection

Set-SfDBConnection

Parameters

-DBConnection<String>

Specifies the database connection string to be tested by the Storefront Service.

Required?	true
Default Value	
Accept Pipeline Input?	false

-LoggingId<Guid>

Specifies the identifier of the high-level operation this cmdlet call forms a part of. Citrix Studio and Director typically create high-level operations. PowerShell scripts can also wrap a series of cmdlet calls in a high-level operation by way of the Start-LogHighLevelOperation and Stop-LogHighLevelOperation cmdlets.

Required?	false
Default Value	
Accept Pipeline Input?	false

-AdminAddress<String>

Specifies the address of a XenDesktop controller the PowerShell snap-in will connect to. You can provide this as a host name or an IP address.

Required?	false
Default Value	Localhost. Once a value is provided by any cmdlet, this value becomes the default.
Accept Pipeline Input?	false

Return Values

Citrix.Fma.Sdk.Utilities.Service.ServiceStatusInfo

The Test-SfDBConnection command returns an object containing the status of the Storefront Service if the connection string of the specified data store were to

be set to the string being tested, together with extra diagnostics information for the specified connection string.

DBRejectedConnection

The database rejected the logon attempt from the Storefront Service. This may be because the service attempted to log on with invalid credentials or because a database has not been installed in the specified location.

InvalidDBConfigured

The expected stored procedures are missing from the database. This may be because the Storefront Service schema has not been added to the database.

DBNotFound

The specified database could not be located with the configured connection string.

DBNewerVersionThanService

The version of the Storefront Service currently in use is incompatible with the version of the Storefront Service schema on the database. Upgrade the Storefront Service to a more recent version.

DBOlderVersionThanService

The version of the Storefront Service schema on the database is incompatible with the version of the Storefront Service currently in use. Upgrade the database schema to a more recent version.

DBVersionChangeInProgress

A database schema upgrade is currently in progress.

OK

The Set-SfDBConnection command would succeed if it were executed with the supplied connection string.

Failed

The Storefront Service has failed.

Unknown

The status of the Storefront Service cannot be determined.

Notes

If the command fails, the following errors can be returned.

Error Codes

InvalidDBConnectionString

The database connection string has an invalid format.

PermissionDenied

You do not have permission to execute this command.

AuthorizationError

There was a problem communicating with the Citrix Delegated Administration Service.

ConfigurationLoggingError

The operation could not be performed because of a configuration logging error.

CommunicationError

There was a problem communicating with the remote service.

ExceptionThrown

An unexpected error occurred. For more details, see the Windows event logs on the controller or the XenDesktop logs.

Examples

-------------------------- EXAMPLE 1 --------------------------

c:\PS>Test-SfDBConnection -DBConnection "Server=serverName\SQLEXPRESS;Initial Catalog = databaseName; Integrated Security = True"

OK
Tests a database connection string for the Storefront Service.

-------------------------- EXAMPLE 2 --------------------------

c:\PS>Test-SfDBConnection -DBConnection "Invalid Connection String"

Invalid database connection string format.
Tests an invalid database connection string for the Storefront Service.

Third party notices

Nov 25, 2015

XenApp and XenDesktop 7.6 may include third party software licensed under the terms defined in the following documents:

- XenApp 7.6 and XenDesktop 7.6 Third Party Notices
- FlexNet Publisher Documentation Supplement: Software Licenses