Citrix Virtual Apps and Desktops service
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Virtual Apps and Desktops service</td>
<td>3</td>
</tr>
<tr>
<td><strong>What’s new</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Known issues</strong></td>
<td>25</td>
</tr>
<tr>
<td><strong>System requirements</strong></td>
<td>26</td>
</tr>
<tr>
<td><strong>Technical security overview</strong></td>
<td>31</td>
</tr>
<tr>
<td><strong>Delivery methods</strong></td>
<td>36</td>
</tr>
<tr>
<td><strong>Install and configure</strong></td>
<td>40</td>
</tr>
<tr>
<td><strong>Get started</strong></td>
<td>45</td>
</tr>
<tr>
<td><strong>Set up resource locations</strong></td>
<td>46</td>
</tr>
<tr>
<td>Microsoft Azure Resource Manager virtualization environments</td>
<td>49</td>
</tr>
<tr>
<td>Citrix Hypervisor virtualization environments</td>
<td>58</td>
</tr>
<tr>
<td>Microsoft System Center Virtual Machine Manager virtualization environments</td>
<td>60</td>
</tr>
<tr>
<td>VMware virtualization environments</td>
<td>63</td>
</tr>
<tr>
<td>Amazon Web Services virtualization environments</td>
<td>69</td>
</tr>
<tr>
<td>Nutanix virtualization environments</td>
<td>78</td>
</tr>
<tr>
<td>Google Cloud Platform virtualization environments</td>
<td>79</td>
</tr>
<tr>
<td>Install Cloud Connectors</td>
<td>89</td>
</tr>
<tr>
<td>Scale and size considerations for Cloud Connectors</td>
<td>92</td>
</tr>
<tr>
<td>Scale and size considerations for Local Host Cache</td>
<td>108</td>
</tr>
<tr>
<td>Create and manage connections</td>
<td>124</td>
</tr>
<tr>
<td>Install VDAs</td>
<td>135</td>
</tr>
<tr>
<td>Install VDAs using the command line</td>
<td>151</td>
</tr>
<tr>
<td>Create machine catalogs</td>
<td>158</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Manage machine catalogs</td>
<td>169</td>
</tr>
<tr>
<td>Azure Quick Deploy</td>
<td>176</td>
</tr>
<tr>
<td>Create Delivery Groups</td>
<td>179</td>
</tr>
<tr>
<td>Manage Delivery Groups</td>
<td>185</td>
</tr>
<tr>
<td>Create Application Groups</td>
<td>201</td>
</tr>
<tr>
<td>Remove components</td>
<td>208</td>
</tr>
<tr>
<td>Upgrade</td>
<td>209</td>
</tr>
<tr>
<td>Print</td>
<td>210</td>
</tr>
<tr>
<td>HDX technologies</td>
<td>211</td>
</tr>
<tr>
<td>Policies</td>
<td>211</td>
</tr>
<tr>
<td>Manage</td>
<td>212</td>
</tr>
<tr>
<td>Autoscale</td>
<td>213</td>
</tr>
<tr>
<td>Configuration Logging</td>
<td>238</td>
</tr>
<tr>
<td>Delegated Administration</td>
<td>241</td>
</tr>
<tr>
<td>Local Host Cache</td>
<td>254</td>
</tr>
<tr>
<td>Scale and size considerations for Local Host Cache</td>
<td>263</td>
</tr>
<tr>
<td>Tags</td>
<td>279</td>
</tr>
<tr>
<td>Zones</td>
<td>287</td>
</tr>
<tr>
<td>Monitor</td>
<td>296</td>
</tr>
<tr>
<td>Site Analytics</td>
<td>297</td>
</tr>
<tr>
<td>Alerts and notifications</td>
<td>306</td>
</tr>
<tr>
<td>Filter data to troubleshoot failures</td>
<td>315</td>
</tr>
<tr>
<td>Monitor historical trends across a Site</td>
<td>317</td>
</tr>
<tr>
<td>Monitor Autoscale-managed machines</td>
<td>324</td>
</tr>
</tbody>
</table>
Troubleshoot deployments 327
Troubleshoot applications 327
Application probing 331
Desktop probing 335
Troubleshoot machines 339
Troubleshoot user issues 346
Diagnose user logon issues 348
Diagnose session startup issues 354
Shadow users 359
Send messages to users 361
Resolve application failures 361
Restore desktop connections 363
Restore sessions 363
Run HDX channel system reports 364
Reset a user profile 364
Delegated Administration and Monitoring 367
Data granularity and retention 371
Citrix Gateway 375
SDKs and APIs 377
February 4, 2019

Introduction

Citrix Virtual Apps and Desktops provides virtualization solutions that give IT control of virtual machines, applications, and security while providing anywhere access for any device. End users can use applications and desktops independently of the device’s operating system and interface.

Using the Citrix Virtual Apps and Desktops service, you can deliver secure virtual apps and desktops to any device, and leave most of the product installation, setup, configuration, upgrades, and monitoring to Citrix. You maintain complete control over applications, policies, and users while delivering the best user experience on any device.

You connect your resources to the service through Citrix Cloud Connector, which serves as a channel for communication between Citrix Cloud and your resource locations. Cloud Connector enables cloud management without requiring any complex networking or infrastructure configuration such as VPNs or IPsec tunnels. Resource locations contain the machines and other resources that deliver applications and desktops to your subscribers.

Who manages what

The following graphic shows the core components in a Citrix Virtual Apps and Desktops service deployment.
Components

As shown in the graphic, Citrix manages the core components in Citrix Cloud. Citrix also takes care of installing and upgrading those components. (This differs from an on-premises Citrix Virtual Apps and Desktops deployment, where you are responsible for installing, managing, and upgrading the core components.)

Your applications and desktops reside in one or more resource locations. You install and manage most components in each resource location. The exceptions are the Citrix Cloud Connectors. You install the Cloud Connectors; Citrix manages them.

The following graphic shows a layer view of the Citrix Virtual Apps and Desktops service components.
Citrix Workspace app is installed on user devices and other endpoints, such as virtual desktops. Citrix Workspace app provides users with secure, self-service access to documents, applications, and desktops from any device, including smartphones, tablets, and PCs. Citrix Workspace app provides on-demand access to Windows, web, and Software as a Service (SaaS) applications. For devices that cannot install Citrix Workspace app software, Citrix Workspace app for HTML5 provides a connection through a HTML5-compatible web browser.

**Citrix Cloud components**

Citrix installs and manages the following components in Citrix Cloud.

**Delivery Controller**

The Delivery Controller is the central control layer component in a deployment. The Controller’s services communicate through the Cloud Connectors in each resource location 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.
- Track which users are logged on and where, which session resources the users have, and if users
Citrix Virtual Apps and Desktops service

need to reconnect to existing applications. This includes managing the state of desktops, starting and stopping them based on demand and administrative configuration.

Data from the Controller services is stored in a Microsoft SQL Server site database. A deployment also uses a Configuration Logging database, plus a monitoring database used by Director.

When the Citrix Cloud is hosted on Microsoft Azure, SQL Server on Azure VMs (IaaS) is supported. Azure SQL (PaaS) Database is not supported.

Citrix license management

License management functionality communicates with the Controller to manage licensing for each user’s session and allocate license files. The customer administrator does not need to configure or manage anything with licensing. All of that work is done automatically in Citrix Cloud.

Citrix Studio

Studio is the management console you use to configure and manage connections, machine catalogs, and Delivery Groups. Studio launches when you select Manage in the Citrix Cloud console.

Citrix Director

Director 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. Displays include:

- Real-time session data from the Broker Service in the Controller, which includes data from the broker agent in the VDA.
- Historical data from the Monitor Service in the Controller.
- Data about HDX traffic (also known as ICA traffic).

Director provides the data when you select Monitor in the Citrix Cloud console.

Workspace configuration

From Workspace configuration in Citrix Cloud, you can:

- Specify which services are integrated with Citrix Workspace.
- Customize the URL that your subscribers use to access their workspace.
- Customize the appearance of subscribers’ workspaces, such as logos, color, and preferences.
- Specify how subscribers authenticate to their workspace, such as using Active Directory or Azure Active Directory.
- Specify external connectivity for resource locations used by your subscribers.
**Citrix StoreFront**

Citrix StoreFront is the predecessor to Citrix Workspace, and is used in on-premises deployments. It offers several similar features to Citrix Workspace, including subscriber access to apps and desktops, authentication, and other subscriber data that ensures consistent experience across devices.

In a service deployment, you can optionally install StoreFront servers in resource locations. Having local stores can help deliver apps and desktops during network outages.

**Citrix Gateway**

When users connect from outside the corporate firewall, Citrix Virtual Apps and Desktops can use Citrix Gateway technology to secure these connections with TLS. The Citrix Gateway or VPX virtual appliance is an SSL VPN appliance deployed in the DMZ. It provides a single secure point of access through the corporate firewall.

Although Citrix installs and manages Citrix Gateway in Citrix Cloud, you can also optionally install Citrix Gateway in resource locations.

**Components in resource locations**

A resource location contains resources required to deliver services to your subscribers (users). You manage these resources from Citrix Cloud. Resource locations contain different resources depending on which Citrix Cloud services you’re using and the services you want to provide to your users.

To interact with Citrix Cloud, each resource location needs Cloud Connectors and access to a Microsoft Active Directory domain.

In a Citrix Virtual Apps and Desktops service deployment, a resource location contains items from the access layer and resource layer:

- Cloud Connectors
- Active Directory domain controller
- Virtual Delivery Agents (VDAs)
- Hypervisors that provision VDAs and store their data, if used
- Citrix Gateway (optional)
- StoreFront servers (optional)

**Cloud Connector**

Every resource location contains at least one Cloud Connector (two or more are recommended for redundancy). A Cloud Connector is the communications channel between the components in the
Citrix Cloud and components in the resource location. In the resource location, the Cloud Connector acts as a proxy for the Delivery Controller in Citrix Cloud.

You install Cloud Connectors from the Citrix Cloud console. Citrix then manages and updates the Cloud Connectors automatically.

**Virtual Delivery Agents (VDAs)**

Each physical or virtual machine that delivers applications and desktops must have a VDA. The VDA registers with a Cloud Connector. After registration, connections are brokered from those resources to users. VDAs establish and manage the connection between the machine and the user device, and apply policies that are configured for the session.

The VDA communicates session information to the Cloud Connector through a broker agent in the VDA. The broker agent hosts multiple plugins and collects real-time data.

VDAs are available 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 desktop operating systems allow only one user to connect to the desktop at a time. Linux VDAs are also available.

Throughout this documentation, “VDA” refers to the agent and the machine on which it is installed.

**Hypervisors and cloud services**

A hypervisor or cloud service contains the VDAs that host applications and desktops.

To provision virtual machines that deliver applications and desktops, you can use:

- **Machine Creation Services**: The MCS technology is built into Studio and is accessed automatically through the Citrix Cloud Console. MCS creates copies of a master image to create and provision VMs.
- **Citrix Provisioning (formerly Provisioning Services)**: The Citrix Provisioning technology streams a master image to user devices. Citrix Provisioning doesn’t require a hypervisor, so you can provision physical machines.
- **Another provisioning tool of your choice**.

Although many deployments use hypervisors, you don’t need one if:

- Your applications and desktops are hosted on physical machines.
- You use Citrix Provisioning to provision VMs.
- You want to deploy Remote PC Access, which enables employees to remotely access their physical PCs.
Active Directory

Although not a Citrix component, Microsoft Active Directory is required for authentication and authorization in any deployment. The Kerberos infrastructure in Active Directory is used to guarantee the authenticity and confidentiality of communications with Citrix Cloud.

Items that help deliver desktops and applications

As part of delivering applications and desktops to users in a production environment, you configure the following items.

Host connection

A host connection enables communication between components in the control plane (Citrix Cloud) and VDAs in a hypervisor or cloud service. Connection specifications include:

- The address and credentials to access the host
- Which tool you use to create VMs
- The storage method to use, and the machines to use for storage
- Which network the VMs will use

Machine catalog

A machine catalog is a collection of virtual or physical machines that have the same operating system type: server or desktop.

If you use VMs, you can create a master image (also known as template) on the hypervisor or cloud service, and install a VDA on the master image. You can also install applications on the master image, if you want them to appear on all machines created from that image and don’t want to virtualize them. Then, you create a catalog using a Citrix tool (MCS or Citrix Provisioning) or your own tools. With Citrix tools, the catalog creation process provisions identical VMs from that image.

If you use your own tools to provision VMs, or if you use physical machines, the catalog creation process adds those machines to the catalog.

For technical details about the Citrix provisioning tools, see Citrix Virtual Apps and Desktops Image Management.

Delivery Group

A Delivery Group specifies:
Citrix Virtual Apps and Desktops service

- One or more machines from a machine catalog.
- Optionally, users who are allowed to access those machines. Alternatively, you can specify users through the Citrix Cloud console.
- Optionally, which applications and desktops users can access. Alternatively, you can specify applications through the Citrix Cloud console.

**Delivering applications and desktops**

*Delivery methods* describes the choices available to deliver applications and desktops to users.

**Service Level Agreement**

The Citrix Virtual Apps and Desktops service (the Service) is designed using industry best practices to achieve cloud scale and a high degree of service availability.

For complete details about Citrix’s commitment for availability of Citrix Cloud services, see the [Service Level Agreement](https://status.cloud.com).

Performance against this goal can be monitored on an ongoing basis at [https://status.cloud.com](https://status.cloud.com).

**Limitations**

The calculation of this Service Level Goal will not include loss of availability from the following causes:

- Customer failure to follow configuration requirements for the Service documented on [https://docs.citrix.com](https://docs.citrix.com).
- Caused by any component not managed by Citrix including, but not limited to, customer controlled physical and virtual machines, customer installed and maintained operating systems, customer installed and controlled networking equipment or other hardware; customer defined and controlled security settings, group policies and other configuration policies; public cloud provider failures, Internet Service Provider failures or other external to Citrix control.
- Service disruption due to reasons beyond Citrix control, including natural disaster, war or acts of terrorism, government action.

**More information**

- Citrix Virtual Apps and Desktops Service diagrams
- Citrix Virtual Apps and Desktops Service Reference Architecture and Deployment Methods
- Technical security overview
- How typical deployments work
Citrix Virtual Apps and Desktops service

- Network ports
- Third-party notices
- System requirements

Features

- HDX technologies
- Remote PC Access: Enable users to log on remotely from anywhere to a physical PC in the office.
- Publish content: Publish an application that is simply a URL or UNC path to a resource
- Server VDI: Deliver a desktop from a server operating system for a single user

Get started

To learn how to set up your deployment, see Install and configure. That summary guides you through the major steps in the process, and provides links to detailed descriptions.

What’s new

October 8, 2019

A goal of Citrix is to deliver new features and product updates to Citrix Virtual Apps and Desktops service customers when they are available. New releases provide more value, so there’s no reason to delay updates. Rolling updates to the service release approximately every three weeks.

This process is transparent to you. Initial updates are applied to Citrix internal sites only, and are then applied to customer environments gradually. Delivering updates incrementally in waves helps ensure product quality and maximize availability.

For details about the Service Level Agreement for cloud scale and service availability, see Service Level Agreement. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

Virtual Delivery Agents (VDAs): VDAs for Windows machines generally release at the same time as the on-premises Citrix Virtual Apps and Desktops product.

- For information about new VDA and HDX features, see the What’s new and Known issues articles for the current on-premises Citrix Virtual Apps and Desktops release.
- For information about VDA platforms and features that are no longer supported, see Deprecation. That article also includes platforms and features that are scheduled to be unsupported in a future release (such as which operating systems support VDA installation).
October 2019

New and enhanced features

Google Cloud Platform. Citrix Virtual Apps and Desktops service now adds support for using Machine Creation Services (MCS) to provision machines on the Google Cloud Platform (GCP). For more information, see Google Cloud Platform virtualization environments.

September 2019

New and enhanced features

VDA support for Windows Virtual Desktop. For supported operating systems and VDA versions see VDAs in a Windows Virtual Desktop environment.

Enhanced power policy. In earlier releases, a VDI machine transitioning to a time period where an action (disconnect action="Suspend" or “Shutdown”) was required remained powered on. This scenario occurred if the machine disconnected during a time period (peak or off-peak times) where no action (disconnect action="Nothing") was required.

Starting with this release, Autoscale suspends or powers off the machine when the specified disconnection time elapses, depending on the disconnect action configured for the destination time period. For details, see Power manage VDI machines transitioning to a different time period with disconnected sessions.

Machine catalogs: Tags. You can now use PowerShell to apply tags to machine catalogs. For details, see Tags on machine catalogs. This feature is being rolled out in phases. It might not yet be activated for your account.

Session startup duration. Monitor now displays the session startup duration divided into Workspace App Session Startup and VDA Session Startup time periods. This data helps you to understand and troubleshoot high session startup duration. Further, the time duration for each phase involved in the session startup helps in troubleshooting issues associated with individual phases. For example, if the Drive Mapping time is high, you can check if all the valid drives are mapped properly in the GPO or script. This feature is available on VDAs 1903 or later. For more information, see Diagnose session startup issues.

August 2019

New and enhanced features

Session Auto Reconnect. The Sessions page on the Trends tab now includes information about the number of auto reconnects. Auto reconnects are attempted when the Session Reliability or Auto Client
Reconnect policies are in effect. The auto reconnect information helps you view and troubleshoot network connections having interruptions, and also analyze networks having a seamless experience. The drilldown provides additional information like Session Reliability or Auto Client Reconnect, time stamps, Endpoint IP, and Endpoint Name of the machine where the Workspace app is installed. This feature is available for Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Receiver for Windows, and Citrix Receiver for Mac. This feature requires VDAs 1906 or later. For more information, see:

- Sessions
- Auto client reconnect policy settings
- Session reliability policy settings
- Session Auto Reconnect

July 2019

New and enhanced features

**Configuration Logging.** You can now use the Remote PowerShell SDK to periodically delete Configuration Logging database content. For details, see [Schedule periodic data deletion](#).

**Autoscale.** Autoscale now provides the flexibility to power manage only a subset of machines in a Delivery Group. This feature can be useful in cloud bursting use cases, where you want to use on-premises resources to handle workloads before cloud-based resources address additional demand (that is, burst workloads). For details, see [Restrict Autoscale to certain machines in a Delivery Group](#).

**Local App Access and URL redirection.** Citrix Studio now lets you add the Add Local App Access Application option to the Studio user interface for your Site by using the PowerShell SDK. For more information, see [Provide access only to published applications](#).

**Operating system name changes.** Operating system names on the Create Machine Catalog > Machine Catalog Setup > Operating System and the Monitor pages have changed:

- Multi-session OS (formerly Server OS): The multi-session OS machine catalog provides hosted shared desktops for a large-scale deployment of standardized Windows multi-session or Linux OS machines.
- Single session OS (formerly Desktop OS): The single session OS machine catalog provides VDI desktops ideal for a variety of different users.

**Citrix Profile Management duration in Profile Load.** Monitor now includes profile processing duration in the Profile Load bar of the Logon duration chart. This is the duration Citrix Profile Management takes to process user profiles. This information helps administrators to troubleshoot high profile load
durations with greater accuracy. This enhancement is available on VDAs 1903 and later. For more information, see Profile Load.

**Desktop probing.** Desktop probing is a feature of the Citrix Virtual Apps and Desktops service. It automates health checks of virtual desktops published on a Site, thereby improving the user experience. To initiate desktop probing, install and configure the Citrix Probe Agent on one or more endpoints. Desktop probing is available for Premium licensed Sites. This feature requires Citrix Probe Agent 1903 or later. For more information, see Desktop Probing.

**Note:**

Citrix Probe Agent now supports TLS 1.2.

---

**June 2019**

**New and enhanced features**

**Restrict by tags.** Tags are strings that identify items such as machines, applications, desktops, Application Groups, and policies. After creating a tag and adding to an item, you can tailor certain operations to apply to only items that have a specified tag. For details, see Application Groups and Tags.

**Email Notifications.** Citrix Virtual Apps and Desktops service sends email notifications related to alerting and probing directly. This eliminates the need to configure the SMTP email server. The Notification Preferences box is enabled by default and Citrix Cloud sends alert notifications to the email addresses provided in the Notification Preferences section. Ensure that the email address ‘donotreplynotifications@citrix.com’ is white-listed in your email setup.

---

**May 2019**

**New and enhanced features**

**Autoscale.** Autoscale is a feature of Citrix Virtual Apps and Desktops service that provides a consistent, high-performance solution to proactively power manage your machines. It aims to balance costs and user experience. Autoscale incorporates the deprecated Smart Scale technology into the Studio power management solution. For more information, see Autoscale. You can monitor the metrics of Autoscale-managed machines from the Trends pages on the Monitor tab. For more information, see Monitor Autoscale-managed machines.
February 2019

New and enhanced features

**Hypervisor alerts monitoring.** Alerts from Citrix Hypervisor and VMware vSphere are now displayed on the Monitor > Alerts tab to help monitor the following states/parameters of hypervisor health:

- CPU usage
- Memory usage
- Network usage
- Hypervisor connection unavailable
- Disk usage (vSphere only)
- Host connection or power state (vSphere only)

For more information, see the Hypervisor alerts monitoring section in Alerts and Notifications.

**Communications over earlier TLS versions.** To improve the security of the Citrix Virtual Apps and Desktops service, Citrix will block any communication over Transport Layer Security (TLS) 1.0 and 1.1 as of March 15, 2019, allowing only TLS 1.2 communications. For details, see TLS versions. For comprehensive guidance, see CTX247067.

**Application Groups.** Application Groups let you manage collections of applications. You can create Application Groups for applications shared across different Delivery Groups or used by a subset of users within Delivery Groups. For details, see Create Application Groups.

**Logon Performance - Profile Drilldown.** The Logon Duration panel on the User Details page within Monitor now includes information on the Profile load phase drill down of the logon process. Profile Drilldown provides useful information about user profiles for the current session that can help administrators troubleshoot high profile load issues. A tool tip with the following user profiles information is displayed:

- Number of files
- Profile size
- Number of large files

A detailed drill down provides information about the individual folders, their size, and the number of files. This feature is available on VDAs 1811 and later. For more information, see Diagnose user logon issues.

**Microsoft RDS license health.** Monitor the Microsoft RDS (Remote Desktop Services) license status on the Machine Details panel on the Machine Details and the User Details page for Server OS machines. An appropriate message is displayed for the license status. You can hover over the info icon to see further details. For more information, see the Microsoft RDS license health section in Troubleshooting Machines.
**Application Probing.** This feature automates the assessment of the health of Virtual Apps published in a Site.

To initiate application probing:

- On one or more endpoint machines, install the Citrix Application Probe Agent
- Configure the Citrix Application Probe Agent with the credentials of Citrix Workspace and Citrix Virtual Apps and Desktops service.
- Configure the applications to be probed, the endpoint machines to run the probe on, and the scheduled probe time in **Monitor > Configuration** of the Citrix Virtual Apps and Desktops service.

The agent tests the launch of selected applications via Citrix Workspace and reports back the probe results on the **Monitor** tab of Citrix Virtual Apps and Desktops service in:

- the Applications page – the last 24-hours’ data and the **Trends > Application Probe Results** page
- the historical probe data along with the stage when the probe failure occurred - Workspace Reachability, WorkspaceAuthentication, WorkspaceEnumeration, ICA download, or Application launch

The failure report is emailed to configured email addresses. You can schedule your application probes to run during off-peak hours across multiple geographical locations, and use the results to proactively troubleshoot issues related to provisioned applications, hosting machines or connections before the users experience them. For more information, see **Application Probing**

### January 2019

**New and enhanced features**

**Delegated Administration with custom scope.** Monitoring now supports custom scope for built-in delegated administrator roles. For more information on the available built-in roles for monitoring and how to assign them, see **Delegated administrator roles.**

### December 2018

**New and enhanced features**

The date after which Citrix will block communication over Transport Layer Security (TLS) 1.0 and 1.1 has changed from December 31, 2018 to January 31, 2019. For details, see **Deprecation of TLS versions.**
November 2018

New and enhanced features

**Machine historical data available using OData API:** Historical data containing machine analytics is now available through the OData API. This data is collected on an hourly basis and rolled up for the day.

- Number of powered on machines (for power managed machines)
- Number of registered machines
- Number of machines in maintenance mode
- Total number of machines

The data is aggregated for the time period during which the Monitoring Service is running. For more information on the usage of the OData API and examples, see [Citrix Monitor Service 7 1808](#). The database schema is available at [Monitor Service Schema](#).

**Logon Performance - Interactive session drilldown:** The Logon Duration panel on the User and Session Details view includes information on the Interactive Session phase of the logon process. The time taken for each of the three subphases (Pre-userinit, Userinit, and Shell) is displayed on the Interactive Session bar as a tooltip. This provides more granular troubleshooting and remediation of this phase of the logon. The cumulative time delay between the subphases and a link to the documentation is also provided. This feature is available on Delivery Controller version 7 1808 and later. The Interactive Session drilldown bar shows the time duration for the current session only. For more information, see [Diagnose user logon issues](#).

**Logon Performance - GPO drilldown:** The Logon Duration panel on the User and Session details view contains the GPO (Group Policy Objects) duration. This is the total time taken to apply the GPOs on the virtual machine during the logon process. Now, you can see the drilldown of each policy applied as per CSEs (Clients-Side Extension) as a tooltip on the GPO bar. For each policy application, the drilldown displays the status and the time taken. This additional information eases troubleshooting and remediation of issues involving high GPO duration. The time durations in the drilldown represent the CSE processing time only and do not add up to the total GPO time. This feature is available on Delivery Controller version 7 1808 and later. For more information, see [Diagnose user logon issues](#).

**Fixes**

Custom report queries saved during monitoring are not available after a Cloud upgrade. [DNA-23420]
October 2018

New and enhanced features

**Applications: Limit per machine.** You can now limit the number of application instances per machine. This limit applies to all machines in the Site. This limit is an addition to the existing application limit for all users in the Delivery Group and the limit per user. This capability is available only through PowerShell, not in Studio. For details, see Configure application limits.

**Windows Server 2019.** You can now install VDAs for Server OS on Windows Server 2019 machines, as noted in System requirements.

September 2018

New and enhanced features

**Delegated Administration.** With Delegated Administration, you can configure the access permissions that all of your administrators need, in accordance with their role in your organization. For details, see Delegated Administration. Monitoring supports allocation of built-in roles; they are currently available with full scope. For more information on the available built-in roles for monitoring and how to assign them, see Delegated administrator roles.

**Configuration Logging.** Configuration Logging allows administrators to keep track of configuration changes and administrative activities. For details, see Configuration Logging.

Several PowerShell cmdlets in the Remote PowerShell SDK that were previously disabled are now enabled, for use with Configuration Logging:

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

**Local Host Cache.** Local Host Cache is now fully available. Local Host Cache enables connection brokering operations to continue when a Cloud Connector in a resource location cannot communicate with Citrix Cloud. For details, see Local Host Cache.

**Citrix Provisioning.** To provision VDAs, you can now use Citrix Provisioning or the existing Machine Creation Services. For Citrix Provisioning information specific to the cloud environment, see Citrix Provisioning managed by Citrix Cloud.
Fixes

In earlier versions, when using Azure on-demand provisioning, all VMs were deleted when powered-off. Now, only pooled VMs are deleted. Persistent (dedicated) VMs are not deleted when powered-off.

August 2018

• New product names

If you’ve been a Citrix customer or partner for a while, you’ll notice new names in our products and in this product documentation. If you’re new to this Citrix product, you might see different names for a product or component.

The new product and component names stem from the expanding Citrix portfolio and cloud strategy. Articles in this product documentation use the following names.

– Citrix Virtual Apps and Desktops: Citrix Virtual Apps and Desktops offers a virtual app and desktop solution, provided as a cloud service and as an on-premises product, giving employees the freedom to work from anywhere on any device while cutting IT costs. Deliver Windows, Linux, web, and SaaS applications or full virtual desktops from any cloud: public, on premises or hybrid. Virtual Apps and Desktops was formerly XenApp and XenDesktop.

– Citrix Workspace app: The Citrix Workspace app incorporates existing Citrix Receiver technology as well as the other Citrix Workspace client technologies. It has been enhanced to deliver additional capabilities to provide end users with a unified, contextual experience where they can interact with all the work apps, files, and devices they need to do their best work. For more information, see this blog post.

– Citrix SD-WAN: NetScaler SD-WAN, a crucial technology for our customers and partners transforming their branch networks and WANs with cloud technology, is now Citrix SD-WAN.

– Citrix Secure Web Gateway: As the Citrix Networking portfolio expands, we’re proud to offer our robust Citrix Secure Web Gateway service, previously known as NetScaler Secure Web Gateway.

– Citrix Gateway: Our robust NetScaler Unified Gateway, which allows secure, contextual access to the apps and data you need to do your best work, is now Citrix Gateway.

– Citrix Content Collaboration and Citrix Files for Windows: The advanced access, collaboration, workflows, rights management, and integration features of ShareFile are now available in the Citrix Content Collaboration component set in our secure, contextual, integrated Citrix Workspace. Citrix Files for Windows allows you to access your Content Collaboration files directly through a mapped drive, providing a native Windows Explorer experience.
Citrix Virtual Apps and Desktops service

- **Citrix Hypervisor**: The technology from XenServer for virtualization infrastructure, based on the XenProject hypervisor, is now Citrix Hypervisor.

Here’s a quick recap:

<table>
<thead>
<tr>
<th>Is</th>
<th>Was</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Virtual Apps and Desktops</td>
<td>XenApp and XenDesktop</td>
</tr>
<tr>
<td>Citrix Workspace app</td>
<td>Incorporates Citrix Receiver and extensive enhancements</td>
</tr>
<tr>
<td>Citrix SD-WAN</td>
<td>NetScaler SD-WAN</td>
</tr>
<tr>
<td>Citrix Secure Web Gateway</td>
<td>NetScaler Secure Web Gateway</td>
</tr>
<tr>
<td>Citrix Gateway</td>
<td>NetScaler Unified Gateway</td>
</tr>
<tr>
<td>Citrix Content Collaboration</td>
<td>ShareFile</td>
</tr>
<tr>
<td>Citrix Files for Windows</td>
<td>ShareFile Desktop App, ShareFile Sync, ShareFile Drive Mapper</td>
</tr>
<tr>
<td>Citrix Hypervisor</td>
<td>XenServer</td>
</tr>
<tr>
<td>Citrix Provisioning</td>
<td>Citrix Provisioning Services</td>
</tr>
</tbody>
</table>

Implementing this transition in our products and their documentation is an ongoing process.

- In-product content might still contain former names. For example, you might see instances of earlier names in console text, messages, and directory/file names.
- It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.
- Related product documentation and other resources (such as videos and blog posts) that are linked from this product’s documentation might still contain former names.
- For Citrix Hypervisor: The new name will be used on the Citrix website and in informational product materials from September 2018. You will also see the new name on the administrator consoles of some Citrix products, such as Citrix Virtual Apps and Desktops. The XenServer product release and technical documentation materials will continue to use XenServer 7.x until early 2019.

Your patience during this transition is appreciated.

For more detail about our new names, see [https://www.citrix.com/about/citrix-product-guide/](https://www.citrix.com/about/citrix-product-guide/).

- **Product and component version number changes**

  Citrix installs and manages most of the Citrix Virtual Apps and Desktops components, so you
won’t be concerned with those version numbers. However, you might see version numbers when installing Cloud Connectors, and when installing or upgrading VDAs in resource locations.

Citrix Virtual Apps and Desktops product and component version numbers are displayed in the format: **YYMM.c.m.b**

- **YYMM** = Year and month when the product or component released. For example, a September 2018 release appears as 1809.
- **c** = Citrix Cloud release number for the month.
- **m** = Maintenance version (if applicable).
- **b** = Build number. This field is shown only on the About page of the component, and in the OS’s feature for removing or changing programs.

For example, **Citrix Virtual Apps and Desktops 1809.1.0** indicates that the component released in September 2018. It is associated with Citrix Cloud release 1 in that month, and is not a maintenance version. Some displays show only the version’s year and month: for example, **Citrix Virtual Apps and Desktop 1809**.

In earlier releases (7.18 and earlier), version numbers were displayed in the format: **7.version**, where version incremented by one for each release. For example, the VDA release following XenApp and XenDesktop 7.17 was 7.18. Earlier releases (7.18 and earlier) will not be updated with the new numbering format.

- **Deprecation of TLS versions.** To improve the security of the Citrix Virtual Apps and Desktops service, Citrix will block any communication over Transport Layer Security (TLS) 1.0 and 1.1, effective December 31, 2018. For details, see **Deprecation of TLS versions**.

- **Google Cloud Platform virtualization environment.** The Citrix Virtual Apps and Desktops service supports the ability to manually power cycle Virtual Apps and Desktops VMs on the Google Cloud Platform (GCP). For more information, see **Google Cloud Platform virtualization environments**.

**July 2018**

- **Export of Filters data.** You can now export real-time monitoring data on the **Monitor > Filters** tab to CSV format files. The export feature is available from the Machines, Sessions, Connections, and Application Instances Filters pages. You can select a predefined custom filter or select suitable filter criteria, choose required columns on the table, and export the data. Data of up to 100,000 records can be exported. The exported CSV files give a comprehensive view of the real-time data, and helps ease analysis of large data sets.
June 2018

- **Azure Resource Manager connections.** In the Studio connection creation wizard, the Azure environment selection on the Connection page includes all Azure Clouds that are valid for your Azure subscription. General availability for Azure US Government Cloud and Azure Germany Cloud replaces the preview versions of those two environments in earlier releases.

May 2018

- **Azure Quick Deploy.** When your resource location uses Azure Resource Manager machines to deliver applications and desktops, you can now choose a deployment method:
  - Full Configuration: This existing method uses the Studio management console, which guides you through creating a machine catalog and then creating a Delivery Group.
  - Azure Quick Deploy: This new option offers a simpler interface that offers faster deployment of apps and desktops.

  For details, see [Azure Quick Deploy](#).

- **Citrix Health Assistant link.** The Machine Details page of an unregistered machine on the Monitoring console now contains a Health Assistant button. Currently, the button links to the Troubleshoot machines article in docs.citrix.com and to the Knowledge Center article, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch where you can download the tool. Citrix Health Assistant is a tool to troubleshoot configuration issues in unregistered VDAs. The tool automates a number of health checks to identify possible root causes for common VDA registration, session launch, and time zone redirection configuration issues.

- **Interactive Session drilldown.** In the monitoring console, the User Details view > Logon Duration panel now includes information on the Interactive Session stage of the logon process. To provide more granular troubleshooting and remediation of this phase of the logon, Interactive Session now has three sub-phases: Pre-userinit, Userinit, and Shell. In this release, hovering over Interactive Session displays a tooltip showing the sub-phases and a link to the documentation. For a description of the sub-phases and how to improve the performance of each phase, see [Diagnose user logon issues](#).

March 2018

- **Application instance prediction (Preview feature).** This is the first monitoring feature based on predictive analytics. Predicting resource usage patterns is important for administrators to organize resources and the required number of licenses on each resource. The Application instance prediction feature indicates the number of hosted application instances that are likely to be launched per Site or Delivery Group over time. Machine learning algorithms based on
data models created with existing historical data are used to do the prediction. Tolerance level indicates the prediction quality.

For more information see Application instance prediction in Director. Submit your feedback regarding the usefulness and usability of this feature in the Citrix Cloud discussion forum.

• Delivery Groups APIs - Tech Preview

The Delivery Groups APIs Tech Preview provides a set of REST APIs that you can use to automate the management of Delivery Groups. The complete set of available APIs can be viewed and tried out in the Citrix Cloud API documentation at https://developer.cloud.com/.

• Web Studio authentication

The service management console on Citrix Cloud now uses a bearer token to authenticate customers. The bearer token is needed to authenticate access to the Delivery Groups REST API.

• Access Monitor Service data using OData Version 4 API (Preview feature)

You can create your customized monitoring and reporting dashboards based on the Monitor Service data by using the OData V.4 endpoint. OData V.4 is based on ASP .Net Web API and supports aggregation queries. Use your Citrix Cloud user name and bearer token to access the data with the V4 endpoint. For more information and examples, see Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.
Citrix Virtual Apps and Desktops service

Share your feedback on the utility of this feature in the Citrix Cloud discussion forum.

Fixes

• You can rename, move, and delete application folders. [#STUD-2376]

January 2018

• **RDS license check.** Creation of machine catalogs containing Windows Server OS machines now includes an automatic RDS license check. Any RDS license issues found are displayed, so that you can take the appropriate steps to prevent a gap in service. For details, see Create machine catalogs.

• **Access to machine console from Monitor.** The Machine Details panel from Monitor now provides access to consoles of machines hosted on the XenServer hypervisor version 7.3. You can now troubleshoot issues inVDAs directly from Monitor. For more information, see Machine Console access in Troubleshoot machines.

December 2017

New and enhanced features

• **Citrix Workspace.** Citrix Workspace is now available for new XenApp and XenDesktop Service customers. For more information, see Workspace Configuration.

• **Applications Analytics.** You can now analyze and monitor the performance of applications efficiently with the new Application Analytics page available from Monitor > Applications tab. The page provides a consolidated view of the health and usage of all applications published on your Site. It shows metrics such as the number of instances per application, and faults and errors associated with the published applications. This feature requires VDAs Version 7.15 or later.

  For more information, see Application Analytics section in Monitor.

November 2017

New and enhanced features

• **Local Host Cache.** Local Host Cache enables connection brokering operations to continue when a Cloud Connector in a resource location cannot communicate with Citrix Cloud. For details, see Local Host Cache.
• **Azure Managed Disks.** Azure Managed Disks are now used by default for MCS-provisioned VMs in Azure Resource Manager environments. Optionally, you can use conventional storage accounts. For details, see Microsoft Azure Resource Manager virtualization environments.

• **Help desk administrator.** When managing service administrators for a Citrix Cloud customer account, you now have a new choice: Help Desk Administrator. A help desk administrator can access the Monitor functions on the service. For details, see Manage.

**Fixes**

• You can now use the service management console wizard to create a Remote PC Access machine catalog. In earlier releases, you had to use a PowerShell cmdlet to create a catalog (as documented in CTX220737). Then, you had to return to the management console to create a Delivery Group. Now, you create the catalog and the Delivery Group sequentially on the management console.

• MCS-created catalogs can use existing Active Directory machine accounts. [#DNA-24566]

• When monitoring a deployment, scrolling in a sorted **Trends > Sessions** table displays accurate results. [DNA-51257]

**More information**

• Known issues.

• For information about third-party software that is included in the service, see Third party notifications.

**Known issues**

September 20, 2019

The Citrix Virtual Apps and Desktops service has the following known issues:

• If you use Azure AD Domain Services: Workspace (or StoreFront) logon UPNs must contain the domain name that was specified when enabling Azure AD Domain Services. Logons cannot use UPNs for a custom domain you create, even if that custom domain is designated as primary.

• When deploying to Azure and creating an MCS catalog version 7.9 or later with write-back cache enabled and the VDA installed on the master image is 1811 or earlier, an error occurs. Also, you cannot create anything related to Personal vDisk for Microsoft Azure. As a workaround, select a different catalog version to deploy to Azure, or disable write-back cache. To disable write-back
cache when you create a catalog, clear the Memory allocated to cache and Disk cache size check boxes on the Machines page.

- The Console link on Monitor > Machine Details does not launch the Machine Console in the Microsoft Edge 44 and Firefox 68 ESR browsers. [DIR-8160]

For issues related to current VDAs, see Known issues.

System requirements

September 30, 2019

Introduction

System requirements components that are not covered here (such as StoreFront, Citrix Workspace app, and Citrix Provisioning) are described in their respective documentation.

For product components and features that you can install on Windows Servers, Server Core and Nano Server installations are not supported, unless specifically noted.

For globalization information, see CTX119253.

Specific recommendations for sizing VMs that deliver desktops and applications cannot be provided because of the complex and dynamic nature of hardware offerings. Every deployment has unique needs. Generally, sizing a Citrix Virtual Apps VM is based on the hardware and not the user workloads (except for RAM; you’ll need more RAM for applications that consume more). The Citrix VDI Handbook and Best Practices contains the latest guidance on VDA sizing.

Remember: In a Citrix Virtual Apps and Desktops service deployment, you don’t need to install or manage the core components (Delivery Controllers, the site database, Studio, and Director).

Cloud Connectors

For complete details, see Cloud Connector Installation.

Virtual Delivery Agent (VDA) for Desktop OS

Supported operating systems:

- Windows 10
  - For edition support, see CTX224843.
Citrix Virtual Apps and Desktops service

- For Citrix known issues with version 1709, see CTX229052.
- Desktop composition redirection and legacy graphics mode are not supported on Windows 10.

Requirements:

- Microsoft .NET Framework 4.7.1 is installed automatically, if it (or a later version) is not already installed.

Remote PC Access uses this VDA, which you install on physical office PCs. This VDA supports Secure Boot for Citrix Virtual Desktops Remote PC Access on Windows 10.

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 supported Windows desktop OS 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.

For Linux VDA information, see the Linux Virtual Delivery Agent articles.

To use the server VDI feature, you can use the command line interface to install a VDA for Windows Desktop OS on Windows Server 2016. See Server VDI for guidance.

For information about installing a VDA on a Windows 7 machine, see Earlier operating systems.

Virtual Delivery Agent (VDA) for Server OS

Supported operating systems:

- Windows Server 2019, Standard and Datacenter Editions
- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions

The installer automatically deploys the following requirements:

- Microsoft .NET Framework 4.7.1 is installed automatically, if it (or a later version) is not already installed.

The installer automatically installs and enables Remote Desktop Services role services, if they are not already installed and enabled. This triggers a restart.
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 versions, the Media Foundation feature is installed through the Server Manager. However, N editions do not include certain media-related technologies; you can obtain that software from Microsoft or a third party.

If Media Foundation is not present on the VDA, these multimedia features do not work:

- Flash Redirection
- Windows Media Redirection
- HTML5 Video Redirection
- HDX Realtime Webcam Redirection

For Linux VDA information, see the Linux Virtual Delivery Agent articles.

For information about installing a VDA on a Windows Server 2008 R2 machine, see Earlier operating systems.

**VDAs in a Windows Virtual Desktop environment**

Supported operating systems:

- Windows 10 multi-session
- Windows 10 single-session
- Windows 7 single-session
- Windows Server 2012 R2 and newer supported versions

Supported VDA versions:

- On supported Windows 10 and Windows Server: Virtual Delivery Agent 1909 or newer supported versions
- On Windows 7: Virtual Delivery Agent 7.15.5000 (version 7.15 with Cumulative Update 5 Early Access Release) or newer supported 7.15 CUs

For information about the Windows Virtual Desktop service, see the Microsoft Azure article Windows Virtual Desktop and the Microsoft Azure documentation.

**Hosts / virtualization resources**

The following host/virtualization resources (listed alphabetically) are supported. Where applicable, the major.minor versions are supported, including updates to those versions. CTX131239 contains the most current version information, plus links to known issues.
• **Amazon Web Services (AWS)**  
  - You can provision applications and desktops on supported Windows server operating systems.  
  - The Amazon Relational Database Service (RDS) is not supported.  
  For more information, see [Amazon Web Services virtualization environments](#).

• **Citrix Hypervisor (formerly XenServer)**  
  [CTX131239](#) contains the most current version information, plus links to known issues.  
  For more information, see [Citrix Hypervisor virtualization environments](#).

• **Google Cloud Platform**  
  For more information, see [Google Cloud Platform virtualization environments](#) and [Deployment Guide](#).

• **Microsoft Azure Classic** *(deprecated)*

• **Microsoft Azure Resource Manager**  
  For more information, see [Microsoft Azure Resource Manager virtualization environments](#).

• **Microsoft System Center Virtual Machine Manager**  
  Includes any version of Hyper-V that can register with the supported System Center Virtual Machine Manager versions.  
  [CTX131239](#) contains the most current version information, plus links to known issues.  
  For more information, see [Microsoft System Center Virtual Machine Manager virtualization environments](#).

• **Nutanix Acropolis**  
  [CTX131239](#) contains the most current version information, plus links to known issues.  
  For more information, see [Nutanix virtualization environments](#).

• **Oracle Cloud Infrastructure (OCI) Classic**  
  For more information, see [Deploying Citrix Cloud XenApp and XenDesktop Service with Oracle Cloud Infrastructure Classic](#).

• **VMware vSphere (vCenter + ESXi)**  
  No support is provided for vSphere vCenter Linked Mode operation.  
  [CTX131239](#) contains the most current version information, plus links to known issues.  
  For more information, see [VMware virtualization environments](#).
Active Directory functional levels

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

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

For more information about Active Directory, see Active Directory.

HDX technologies

For specific HDX feature support and requirements, see HDX.

Universal Print Server

The Universal Print Server comprises client and server components. The UpsClient component is included in the VDA installation. You install the UpsServer component on each print server where shared printers reside that you want to provision with the Citrix Universal Print Driver in user sessions.

The UpsServer component is supported on:

- Windows Server 2016
- Windows Server 2012 R2 and 2012

Requirement: Microsoft Visual C++ 2013 Runtime, 32- and 64-bit

For VDAs for Windows Server OS, user authentication during printing operations requires the Universal Print Server to be joined to the same domain as the VDA.

Standalone client and server component packages are also available for download.

For more information, see Provision printers.

Other

StoreFront 3.0.1 is the minimum supported version with this release. To use the zone preference feature, you must be using minimum StoreFront 3.7 and Citrix Gateway (formerly Netcaler Gateway) 11.0-65.x.

When using Citrix Provisioning (formerly Provisioning Services) with this release, the minimum supported Provisioning Services version is 7.0.

The Microsoft Group Policy Management Console (GPMC) is required if you store Citrix policy information in Active Directory rather than the Site Configuration database. The machine on which you
install CitrixGroupPolicyManagement_x64.msi must have Visual Studio 2015 runtime installed. For more information, see the Microsoft documentation.

Multiple network interface cards are supported.

Mixed DPIs with multi-monitors. The use of different DPIs between monitors is not supported. You can verify the DPI (% scaling) using Windows Control Panel > Display options. If using a Windows 8.1 or Windows 10 client device, enabling Let me choose one scaling level for all my displays in the Windows Control Panel > Display options will configure the monitors appropriately. For more information, see CTX201696.

Technical security overview

April 25, 2019

Security overview

This document applies to all the Citrix Virtual Apps and Desktops services hosted in Citrix Cloud, including Citrix Virtual Apps Essentials and Citrix Virtual Desktops Essentials.

Citrix Cloud manages the operation of the control plane for Citrix Virtual Apps and Desktops environments. This includes the Delivery Controllers, management consoles, SQL database, license server, and optionally StoreFront and Citrix Gateway (formerly NetScaler Gateway). The Virtual Delivery Agents (VDAs) hosting the apps and desktops remain under the customer’s control in the data center of their choice, either cloud or on-premises. These components are connected to the cloud service using an agent called the Citrix Cloud Connector. If customers elect to use Citrix Workspace, they may also choose to use the Citrix Gateway Service instead of running Citrix Gateway within their data center. The diagram below illustrates the service and its security boundaries.
Data flow

As the components hosted by the cloud service do not include the VDAs, the customer’s application data and golden images required for provisioning are always hosted within the customer setup. The control plane has access to metadata, such as usernames, machine names, and application shortcuts, restricting access to the customer’s Intellectual Property from the control plane.

Data flowing between the cloud and customer premises uses secure TLS connections over port 443.

Data isolation

The Citrix Virtual Apps and Desktops service stores only the metadata needed for the brokering and monitoring of the customer’s applications and desktops. Sensitive information, including master images, user profiles, and other application data remain on the customer premises or in their subscription with a public cloud vendor.

Service editions

The capabilities of the Citrix Virtual Apps and Desktops service vary by edition. For example, Citrix Virtual Apps Essentials only supports Citrix Gateway service and Citrix Workspace. Consult product documentation to learn more about supported features.

Credential handling

The service handles four types of credentials:
Citrix Virtual Apps and Desktops service

- **User Credentials:** When using a customer-managed StoreFront, user credentials are encrypted by the Citrix Cloud Connector using AES-256 encryption and a random one-time key generated for each launch. The key is never passed into the cloud, and returned only to Citrix Workspace app. This key is then passed to the VDA directly by Citrix Workspace app to decrypt the user password during session launch for a single sign-on experience. The entire flow is shown in the figure below.

![Citrix Cloud Connector Diagram](image)

- **Administrator Credentials:** Administrators authenticate against Citrix Cloud, which uses the sign-on system from Citrix Online. This generates a one-time signed JSON Web Token (JWT) which gives the administrator access to the Citrix Virtual Apps and Desktops service.

- **Hypervisor Passwords:** On-premises hypervisors that require a password for authentication have a password generated by the administrator and directly stored encrypted in the SQL database in the cloud. Peer keys are managed by Citrix to ensure that hypervisor credentials are only available to authenticated processes.

- **Active Directory (AD) Credentials:** Machine Creation Services uses the connector for creating machine accounts in a customer’s AD. Because the machine account of the connector has only read access to AD, the administrator is prompted for credentials for each machine creation or deletion operation. These credentials are stored only in memory and only held for a single provisioning event.

**Deployment considerations**

Citrix recommends that users consult the published best practices documentation for deploying Citrix Gateway applications and VDAs within their environments. Additional considerations regarding on-premises StoreFront deployment and network connectivity are as follows:
Citrix Cloud Connector network access requirements

The Citrix Cloud Connectors require only port 443 outbound traffic to the internet, and may be hosted behind an HTTP proxy.

- The communication used in Citrix Cloud for HTTPS is TLS 1.0, 1.1, or 1.2. (See Deprecation of TLS versions below for in-progress changes.)
- Within the internal network, the connector needs access to the following for the Citrix Virtual Apps and Desktops service:
  - VDAs (port 80, both inbound and outbound) plus 1494 and 2598 inbound if using Citrix Gateway service
  - StoreFront servers (port 80 inbound)
  - Citrix Gateways, if configured as a STA (port 80 inbound)
  - Active Directory domain controllers
  - Hypervisors (outbound only; see hypervisor documentation for specific ports)

Traffic between the VDAs and Cloud Connectors is encrypted using Kerberos message-level security.

Customer-managed StoreFront

A customer-managed StoreFront offers greater security configuration options and flexibility for deployment architecture, including the ability to maintain user credentials on-premises. The StoreFront can be hosted behind the Citrix Gateway to provide secure remote access, enforce multifactor authentication, and add other security features.

Citrix Gateway service and Citrix Workspace

Using the Citrix Gateway service avoids the need to deploy Citrix Gateway within customer data centers. To use the Citrix Gateway Service, it is a prerequisite to use the StoreFront service delivered from Citrix Cloud. The data flow when using Citrix Gateway service is shown in the figure below.

Note: This diagram shows the logical data flows. All TLS connections between the Cloud Connector and Citrix Cloud are initiated from the Cloud Connector to the Citrix Cloud. No in-bound firewall port mapping is required.
Citrix Virtual Apps and Desktops service

**Deprecation of TLS versions**

To improve the security of the Citrix Virtual Apps and Desktops service, Citrix began blocking any communication over Transport Layer Security (TLS) 1.0 and 1.1 as of March 15, 2019.

Important:
See [CTX247067](#) for the most current and comprehensive guidance for all affected Citrix Cloud services.

**Upgrade to the latest Citrix Receiver or Citrix Workspace app**

To ensure successful connection to Citrix Workspace from user endpoint devices, the installed Citrix Receiver version must be equal to or greater than those listed below, which support TLS 1.2.

<table>
<thead>
<tr>
<th>Receiver</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>4.2.1000</td>
</tr>
<tr>
<td>Mac</td>
<td>12.0</td>
</tr>
<tr>
<td>Linux</td>
<td>13.2</td>
</tr>
<tr>
<td>Android</td>
<td>3.7</td>
</tr>
<tr>
<td>iOS</td>
<td>7.0</td>
</tr>
<tr>
<td>Chrome/HTML5</td>
<td>Latest (Browser must support TLS 1.2)</td>
</tr>
</tbody>
</table>

To upgrade to the latest Citrix Receiver version, go to [https://www.citrix.com/products/receiver/](https://www.citrix.com/products/receiver/).
Alternatively, you can upgrade to our new Citrix Workspace app, which uses TLS 1.2. Learn more. To download the Citrix Workspace app, go to [https://www.citrix.com/downloads/workspace-app/](https://www.citrix.com/downloads/workspace-app/).
[CTX247067](#) describes how to retrieve a list of Citrix Receivers that are connecting to your Citrix Cloud environment for the Citrix Virtual Apps and Desktops service.

**If you need to continue using TLS 1.0 or TLS 1.1**

If you need to continue using TLS 1.0 or 1.1 (for example, if you are using a thin client based on an earlier version of Receiver for Linux), install a StoreFront in your resource location and have all of the Citrix Receivers point to it.
Provisioning

All connections to Citrix Cloud services from Citrix Cloud Connectors require TLS 1.2. Citrix Provisioning and Machine Creation Services will allow TLS 1.0, 1.1, and TLS 1.2 connections by default (no action required) until later this year when they will change to TLS 1.2 only.

Optional: If your security policy requires strict enforcement of TLS 1.2 connections, make the registry setting changes described in CTX247067 on each of your Citrix Cloud Connectors.

More information

See the following resources for more security information:

- Citrix security site: https://www.citrix.com/security
- Secure Deployment Guide for NetScaler
- Security considerations and best practices
- Smart cards
- Transport Layer Security (TLS)

Note:
This document is intended to provide the reader with an introduction to and overview of the security functionality of Citrix Cloud; and to define the division of responsibility between Citrix and customers with regard to securing the Citrix Cloud deployment. It is not intended to serve as a configuration and administration guidance manual for Citrix Cloud or any of its components or services.

Delivery methods

September 28, 2018

A single delivery method will likely not meet all of your requirements.

You can consider several application delivery methods. Choosing the appropriate method helps improve scalability, management, and user experience.

- **Installed app**: The application is part of the base desktop image. The install process involves dll, exe, and other files copied to the image drive in addition to registry modifications. For details, see Create machine catalogs.
- **Streamed app (Microsoft App-V)**: The application is profiled and delivered to the desktops across the network on-demand. Application files and registry settings placed in a container on the virtual desktop and isolated from the base operating system and each other, which helps to address compatibility issues. For details, see App-V.
Citrix Virtual Apps and Desktops service

- **Layered app (Citrix App Layering):** Each layer contains a single application, agent, or operating system. By integrating one OS layer, one platform layer (VDA, Citrix Provisioning agent) and many application layers, an administrator can easily create new, deployable images. Layering simplifies ongoing maintenance, as an OS, agent and application exists in a single layer. When you update the layer, all deployed images containing that layer are updated. See [Citrix App Layering](#).

- **Hosted Windows app:** An application installed on a multi-user Citrix Virtual Apps host and deployed as an application and not a desktop. A user accesses the hosted Windows app seamlessly from the VDI desktop or endpoint device, hiding the fact that the app is executing remotely. For details, see [Create Delivery Groups](#).

- **Local app:** An application deployed on the endpoint device. The application interface appears within the user’s hosted VDI session even though it executes on the endpoint. For details, see [Local App Access and URL redirection](#).

For desktops, you can consider Citrix Virtual Apps published desktops or VDI desktops.

### Citrix Virtual Apps published apps and desktops

Use server OS machines to deliver Citrix Virtual Apps published apps and published desktops.

**Use case:**

- You want inexpensive server-based delivery to minimize the cost of delivering applications to many 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 can include task workers such as call center operators and retail workers, or users that share workstations.
- Application types: any application.

**Benefits and considerations:**

- Manageable and scalable solution within your data center.
- 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.
- 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:

- Application processing takes place on hosting machines, rather than on the user devices. The hosting machine can be a physical or a virtual machine.
- Applications and desktops reside on a server OS machine.
- Machines become available through machine catalogs.
- Machines from machine catalogs are organized into Delivery Groups that deliver the same set of applications to groups of users.
- Server OS machines support Delivery Groups that host either desktops or applications, or both.

Session management and assignment:

- 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 more applications, no additional sessions are required because a user can run multiple applications 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.

- 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.

VM hosted apps

Use desktop OS machines to deliver VM hosted applications

Use case:

- You want a client-based application delivery solution that is secure, provides centralized management, and supports many users per host server. You want to provide those 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 offline 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.

Benefits and considerations:
Applications and desktops on the master image are securely managed, hosted, and run on machines within your data center, 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.

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 can increase the amount of server resources for processing applications and increase the amount of storage for users’ personal vDisks.

User experience:

- The same seamless application experience as hosting shared applications on Server OS machines.

Process, host, and deliver applications:

- The same as server OS machines except they are virtual desktop OS machines.

Session management and assignment:

- 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.
- Within a Delivery Group, when users log on they can access either a statically assigned machine (each time the user logs on to the same machine), or a randomly assigned machine that is selected based on session availability.

VDI desktops

Use desktop OS machines to deliver Citrix Virtual Desktops VDI desktops.

VDI desktops are hosted on virtual machines and provide each user with a desktop operating system. VDI desktops require more resources than Citrix Virtual Apps published desktops, but do not require that applications installed on them support server-based operating systems. Also, depending on the type of VDI desktop you choose, these desktops can be assigned to individual users. This allows users a high level of personalization.

When you create a machine catalog for VDI desktops, you create one of these types of desktops:

- **Random non-persistent desktop, also known as pooled VDI desktop**: Each time a user logs on to one of these desktops, that user connects to a desktop selected from a pool of desktops.
That pool is based on a single master image. All changes to the desktop are lost when the machine restarts.

- **Static non-persistent desktop**: During the first logon, a user is assigned a desktop from a pool of desktops. (Each machine in the pool is based on a single master image.) After the first use, each time a user logs on to use one of these desktops, that user connects to the same desktop that was assigned on first use. All changes to the desktop are lost when the machine restarts.

- **Static persistent desktop**: Unlike other types of VDI desktops, users can fully personalize these desktops. During the first logon, a user is assigned a desktop from a pool of desktops. Subsequent logons from that user connect to the same desktop that was assigned on first use. Changes to the desktop are retained when the machine restarts.

**Install and configure**

April 25, 2019

Use the following sequence to set up your Citrix Virtual Apps and Desktops service deployment. Review the entire process before starting the deployment, so you’ll know what to expect. Links are provided to product documentation and videos.

If you’re not familiar with the components and terminology used in a Citrix Virtual Apps and Desktops deployment, see [Citrix Virtual Apps and Desktops service](#).

Learn about product name changes.

**Get started**

Get started by signing up for a Citrix account and requesting a Citrix Virtual Apps and Desktops service trial.

**Set up a resource location and install Cloud Connectors**

Resource locations contain infrastructure servers (such as Active Directory and Citrix Cloud Connectors), and the machines that deliver apps or desktops to users.

- Begin the setup sequence by configuring your host hypervisor or cloud service, and Active Directory: [Set up Resource locations](#).
- Continue the resource location setup: [Install Cloud Connectors](#).

Here’s a video about how to install Cloud Connectors.
Create a connection to the resource location

After you add a resource location, use the Studio management console to create a connection from the service’s control plane to the resource location.

If you’re deploying a simple proof of concept, this step isn’t necessary.

Install VDAs

Each machine that delivers applications and desktops to users must have a Citrix Virtual Delivery Agent (VDA) installed on it. If you’re using a master image to provision VMs, install a VDA on the master image.

• For installation guidance, see Install VDAs. In addition to step-by-step guidance, that article contains technical information about VDAs, and describes the available VDA installers.
• For command-line VDA installation guidance, see Install VDAs using the command line.

For a Remote PC Access deployment, install a VDA for Desktop OS on each physical office PC. You can use your existing Electronic Software Distribution (ESD) methods.
If you’re deploying a simple proof of concept, simply download and install a VDA on one machine.

Here’s a video about how to download and install a VDA.

For a full deployment, you can use Citrix tools to provision a machine catalog containing multiple machines.

You create a master image on your hypervisor or cloud service to be used for the provisioning. In addition to installing apps or desktops on the master image, you install a VDA. Each machine that is provisioned using that master image contains that VDA.

Creating a master image is described in Create machine catalogs.

**Create a machine catalog**

After you create a connection to your resource location, the Studio workflow guides you to create a machine catalog. A catalog contains physical or virtual machines that deliver the apps or desktops to your users.

If you are using Azure Resource Manager to host your resources, you can optionally use the Azure Quick Deploy deployment method, instead of the Full Configuration method shown in the video below. For
Citrix Virtual Apps and Desktops service

details, see Azure Quick Deploy.

Here's a video about how to create a machine catalog.

The product documentation also describes how to create and use a master image to create a catalog of machines provisioned with a Citrix tool.

**Create a Delivery Group**

After you create your first machine catalog, the Studio workflow guides you to create a Delivery Group.

A Delivery Group specifies which machines can be used from a selected machine catalog. You can specify which users can use those machines, and the applications available on those machines. Alternatively, you can specify users and applications through Citrix Cloud library offerings, rather than directly in a Delivery Group.

Here's a video about how to create a Delivery Group.
Launch applications and desktops

After you complete the preceding steps, publishing occurs automatically. The applications and desktops that you specified are available to users in their workspace. A user simply navigates to the workspace URL and selects an application or desktop, which launches immediately.

As an administrator, you can find the workspace URL in two places:

- From the Citrix Cloud console, select **Workspace Configuration** from the menu in the upper left corner. For more information, see **Workspace configuration**.
- From the Citrix Virtual Apps and Desktops service welcome page, the workspace URL appears at the bottom of the page.

Here’s a short video about launching applications and desktops from your workspace.
Get started

July 9, 2019

When you evaluate or purchase the Citrix Virtual Apps and Desktops service, the Citrix Service Operations team provides ongoing onboarding help. That team also communicates with you to ensure that the core Citrix Virtual Apps and Desktops service is running and configured correctly.

The onboarding steps are:

1. Sign up for a Citrix account and request a Citrix Virtual Apps and Desktops service trial.
2. Discuss integration requirements with Citrix.
3. Complete settings in the Citrix Cloud portal.

To sign up for a Citrix account and request a trial, contact your Citrix Sales Representative. When you’re ready to proceed, go to https://onboarding.cloud.com.

After you log on, in the Citrix Virtual Apps and Desktops service tile, click Request Trial. The text changes to Trial Requested. You will receive an email when your trial is available.
While waiting for the trial, you can review the information referenced in Where to go next. Although Citrix hosts and delivers your Citrix Virtual Apps and Desktops service solution, you manage the machines that deliver applications and desktops, plus the applications and users. You can spend this time setting up the infrastructure to your corporate services, such as Active Directory.

When you are authorized to access the trial, the text on the Citrix Virtual Apps and Desktops service tile changes to Manage.

When you click Manage, a 1-2-3 configuration workflow opens in the Studio management console. However, before you can proceed with that workflow, set up your resource location (or finish setting it up) by adding Citrix Cloud Connectors.

If you currently subscribe to a different Citrix Virtual Apps and Desktops service

Your Citrix Cloud account allows you to subscribe to only one of the Citrix Virtual Apps and Desktops services at a time (for example, Citrix Virtual Apps and Desktops OR Citrix Managed Desktops, but not both). If you currently subscribe to a service, and want to subscribe to this service, you must either:

- Subscribe to this service using a different Citrix Cloud account.
- Decommission the service you already have.

For guidance, see CTX239027.

Where to go next

- If you haven’t already set up your hypervisor or cloud service, or Active Directory, see Set up a resource location.
- If your host environment and Active Directory are already set up, see Create a connection.
- To review the entire configuration process, see Install and configure.

Set up resource locations

September 26, 2019

Setting up a resource location begins with the following tasks:

- Set up your host environment (hypervisor or cloud service).
- Set up your Active Directory domain.
About resource locations

If you’re not familiar with resource locations, review this information.

What’s in a resource location

Resource locations contain the resources required to deliver applications and desktops to users. You manage those items from Citrix Cloud and the Studio console. Typically, resources include:

- Active Directory domain controller
- Hypervisors or cloud services, known as hosts
- Virtual Delivery Agents (VDAs)
- Citrix Gateway (optional): To enable secure external access to the applications and desktops offered to users, add a Citrix Gateway VPX appliance to the resource location and set up Citrix Gateway (formerly NetScaler Gateway).
- Citrix StoreFront servers (optional)

To communicate with Citrix Cloud, every resource location must contain a Citrix Cloud Connector. At least two Cloud Connectors per resource location is recommended, for availability.

A resource location is considered a zone in a Citrix Virtual Apps and Desktops service environment.

Where to place resource locations

A resource location can be anywhere you need it: in a public cloud, private cloud, or an on-premises datacenter. You can set up multiple resource locations to meet your company’s specific needs. Planning where to place a resource location can depend on:

- Proximity to users
- Proximity to data
- Scale requirements
- Security attributes

For example, a resource location in your head office’s data center might serve users that must be close to the data. Another resource location in a public cloud might serve global users. Or, resource locations in branch offices might provide applications that are best served near the branch workers. Finally, restricted applications might be placed in a separate resource location, restricting visibility to other resources and users without having to adjust other resource locations.

Host requirements

The hypervisor or cloud service where you provision VMs that deliver apps or desktops to users might have unique permission or setup requirements.

- If the hypervisor or cloud service requires virtual networks or other items, follow the guidance in its documentation.
Citrix Virtual Apps and Desktops service

- Create the appropriate virtual private cloud (VPC) or virtual networks for the machines you’ll add to your resource location, if needed. For example, when using AWS, set up a VPC with public and private subnets.
- Create the appropriate rules to secure inbound and outbound internet traffic, as well as traffic between machines in the virtual network. For example, when using AWS, ensure the VPC’s security group has the appropriate rules configured so that machines in the VPC are accessible only to the IP addresses you specify.

Review the article for the host type you’re using.

- Microsoft System Center Virtual Machine Manager virtualization environments
- Microsoft Azure Resource Manager virtualization environments
- Amazon Web Services (AWS) virtualization environments
- Citrix Hypervisor virtualization environments
- VMware virtualization environments
- Nutanix virtualization environments
- Google Cloud Platform virtualization environments

Active Directory

Provision a Windows server, install Active Directory Domain Services, and promote it to a domain controller. For guidance, see the Microsoft Active Directory documentation.

- You must have at least one domain controller running Active Directory Domain Services.
- Do not install any Citrix components on a domain controller.
- Do not use a forward slash (/) when specifying Organizational Unit names in Studio.

For technical details, see:

- System requirements lists the supported Active Directory functional levels
- Active Directory contains Citrix support details
- Supported Active Directory functional levels

Add a resource location in Citrix Cloud

To add a resource location:

1. Sign in to Citrix Cloud.
2. In the upper left menu, select Resource Locations.
3. If you have not already installed a Citrix Cloud Connector, you are prompted to download one. Follow the guidance in Install Cloud Connectors.
4. After you’ve installed a Cloud Connector (preferably at least two), back in the Citrix Cloud console, enter a name for the resource location and then click Save.
Where to go next

Install Cloud Connectors

To review the entire configuration process, see Install and configure.

Microsoft Azure Resource Manager virtualization environments

April 10, 2019

Follow the guidance in this article when using Microsoft Azure Resource Manager to provision virtual machines in your Citrix Virtual Apps or Citrix Virtual Desktops service deployment.

We assume you are familiar with the following:


Azure Disk Encryption is not supported when using Machine Creation Services.

Azure on-demand provisioning

When you use MCS to create machine catalogs in Azure Resource Manager, the Azure on-demand provisioning feature:

- Reduces your storage costs
- Provides faster catalog creation
- Provides faster virtual machine (VM) power operations

For the administrator, on-demand provisioning introduces no differences in the Studio procedures for creating host connections and MCS machine catalogs. The differences lie in how and when resources are created and managed in Azure, and VM visibility in the Azure portal.

Before Azure on-demand provisioning was used with Citrix Virtual Apps and Desktops, when MCS created a catalog, the VMs were created in Azure during the provisioning process.

With Azure on-demand provisioning, VMs are created only when Citrix Virtual Apps and Desktops initiates a power-on action, after the provisioning completes. A VM is visible in the Azure portal only when it is running. (In Studio, VMs are visible, if they’re running.)
Citrix Virtual Apps and Desktops service

When you create an MCS catalog, the Azure portal displays the resource groups, network security group, storage accounts, network interfaces, base images, and identity disks. The Azure portal does not show a VM until Citrix Virtual Apps and Desktops initiates a power-on action for it. (Then, the VM’s status in Studio changes to On.)

- For a pooled machine, the operating system disk and write-back cache exist only when the VM exists. The cache can result in significant storage savings if you routinely shut down machines (for example, outside of working hours).
- For a dedicated machine, the operating system disk is created the first time the VM is powered on. It remains in storage until the machine identity is deleted.

When Citrix Virtual Apps and Desktops initiates a power-off action for a VM, that machine identity is deleted in Azure. It no longer appears in the Azure portal. (In Studio, the VM’s status changes to Off.)

Catalogs created before on-demand provisioning
If you have machine catalogs that were created before Citrix Virtual Apps and Desktops supported the Azure on-demand provisioning feature (mid-2017), VMs in those catalogs are visible in the Azure portal if they’re running. You cannot convert those VMs to on-demand machines.

To take advantage of the performance enhancements and storage cost benefits of on-demand provisioning, create catalogs using MCS.

Azure managed disks

Azure Managed Disks is an elastic disk storage system you can use with MCS-created machine catalogs, as an alternative to using conventional storage accounts.

The managed disks feature hides the complexity of creating and managing storage accounts, and provides a simple scalable and highly available solution for creating and managing disks. You can use managed disks as master images, in addition to VMs. Using managed disks can improve machine catalog creation and update time. (For more information, see Learn about Managed Disks.)

By default, a machine catalog uses managed disks. You can override the default when you create the catalog.

When I/O optimization is configured (which uses three disks per VM), you can provision up to 3,333 VMs per subscription. When I/O optimization is not configured (which uses two disks per VM), you can provision up to 5,000 VMs disks in a subscription. (The managed disks feature allows you to create up to 10,000 VM disks in a subscription.)

Using managed disks

When you create a machine catalog in Studio, the Master Image page of the catalog creation wizard lists managed disks, in addition to VMs and VHDs. (Not all Azure regions support the managed disks...
Catalog creation time is optimized when the image and catalog are in the same region.

The managed disks feature does not currently support copying disks between Azure regions. If you select an image in a region other than where MCS provisions the catalog, the image is copied to a VHD in a conventional storage account in the catalog’s region. It is then converted back to a managed disk.

On the Storage and License Types page of the catalog creation wizard, you can select a check box to use conventional storage accounts instead of managed disks. This check box is disabled when you are provisioning in an Azure region that does not support managed disks.

Create a connection to Azure Resource Manager

Create and manage connections describes the wizards that create a connection. The following information covers details specific to Azure Resource Manager connections.

Considerations:

- Service principals must have been granted contributor role for the subscription.
- When creating the first connection, Azure prompts you to grant it the necessary permissions. For future connections you must still authenticate, but Azure remembers your previous consent and does not display the prompt again.
- Accounts used for authentication must be a co-administrator of the subscription.
- The account used for authentication must be a member of the subscription’s directory. There are two types of accounts to be aware of: ‘Work or School’ and ‘personal Microsoft account.’ SeeCTX219211 for details.
- While you can use an existing Microsoft account by adding it as a member of the subscription’s directory, there can be complications if the user was previously granted guest access to one of the directory’s resources. In this case, they might have a placeholder entry in the directory that does not grant them the necessary permissions, and an error is returned. One way to rectify this is to remove the resources from the directory and add them back explicitly. However, exercise this option carefully, because it has unintended effects for other resources that account can access.
- There is a known issue where certain accounts are detected as directory guests when they are actually members. Configurations like this typically occurs with older established directory accounts. Workaround: add a new account to the directory, which will take the proper membership value.
- Resource groups are simply containers for resources, and they can contain resources from regions other than their own region. This can potentially be confusing if you expect all of the resources displayed in a resource group’s region to be available.
- Ensure your network and subnet are large enough to host the number of machines you require. This may require some foresight, but Microsoft helps you specify the right values, with guidance.
about the address space capacity.

There are two ways to establish a host connection to Azure Resource Manager:

- Authenticate to Azure Resource Manager to create a service principal.
- Use the details from a previously created service principal to connect to Azure Resource Manager.

**Authenticate to Azure Resource Manager to create a service principal**

Before you start, ensure:

- You have a user account in your subscription’s Azure Active Directory tenant.
- The Azure AD user account is also a co-administrator for the Azure subscription you want to use for provisioning resources.

In the Add Connection and Resources wizard:

1. On the **Connection** page, select the **Microsoft Azure** connection type and your Azure environment.
2. On the **Connection Details** page, enter your Azure subscription ID and a name for the connection. The connection name can contain 1–64 characters, and cannot contain only blank spaces or the characters \ / : # . * ? = <> | + [ ] { } " ’ ( ) . After you enter the subscription ID and connection name, the **Create new** button is enabled.
3. Enter the Azure Active Directory account username and password.
4. Click **Sign in**.
5. Click **Accept** to give Citrix Virtual Apps and Desktops the listed permissions. Citrix Virtual Apps and Desktops creates a service principal that allows it to manage Azure Resource Manager resources on behalf of the specified user.
6. After you click **Accept**, you are returned to the **Connection** page in Studio. Notice that when you successfully authenticate to Azure, the **Create new**, and **Use existing** buttons are replaced with **Connected**, and a green check mark indicates the successful connection to your Azure subscription.
7. Indicate which tools to use to create the virtual machines, and then click **Next**. (You cannot progress beyond this page in the wizard until you successfully authenticate with Azure and accept giving the required permissions.

Resources comprise the region and the network.

- On the **Region** page, select a region.
- On the **Network** page,
  - Type a 1–64 character resources name to help identify the region and network combination in Studio. A resource name cannot contain only blank spaces, and cannot contain the characters \ / : # . * ? = <> | + [ ] { } " ’ ( ) .
Select a virtual network and resource group pair. (Since you can have more than one virtual network with the same name, pairing the network name with the resource group provides unique combinations.) If you selected a region on the previous page that does not have any virtual networks, you need to return to that page and select a region that has virtual networks.

Complete the wizard.

Use the details from a previously created service principal to connect to Azure Resource Manager

To create a service principal manually, connect to your Azure Resource Manager subscription and use the PowerShell cmdlets provided in the following sections.

Prerequisites:

- **$SubscriptionId**: Azure Resource Manager SubscriptionID for the subscription where you want to provision VDAs.
- **$AADUser**: Azure AD user account for your subscription’s AD tenant. Make the $AADUser the co-administrator for your subscription.
- **$ApplicationName**: Name for the application to be created in Azure AD.
- **$ApplicationPassword**: Password for the application. You use this password as the application secret when creating the host connection.

To create a service principal:

1. Connect to your Azure Resource Manager subscription.
   
   `Login-AzureRmAccount`

2. Select the Azure Resource Manager subscription where you want to create the service principal.

   `Select-AzureRmSubscription -SubscriptionID $SubscriptionId;`

3. Create the application in your AD tenant.

   ```
   $AzureADApplication = New-AzureRmADApplication -DisplayName $ApplicationName -HomePage "https://localhost/$ApplicationName" -IdentifierUris $ApplicationName -Password $ApplicationPassword
   ```

4. Create a service principal.

   `New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.ApplicationId`

5. Assign a role to the service principal.

   `New-AzureRmRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.ApplicationId -scope /subscriptions/$SubscriptionId`
6. From the output window of the PowerShell console, note the ApplicationId. You provide that ID when creating the host connection.

In the Add Connection and Resources wizard:

1. On the Connection page, select the **Microsoft Azure** connection type and your Azure environment.
2. On the **Connection Details** page, enter your Azure subscription ID and a name for the connection. (The connection name can contain 1–64 characters, and cannot contain only blank spaces, or non-ASCII or special characters.
3. Click **Use existing**. Provide the subscription ID, subscription name, authentication URL, management URL, storage suffix, Active Directory ID or tenant ID, application ID, and application secret for the existing service principal. After you enter the details, the **OK** button is enabled. Click **OK**.
4. Indicate which tools to use to create the virtual machines, and then click **Next**. The service principal details you provided are used to connect to your Azure subscription. (You cannot progress beyond this page in the wizard until you provide valid details for the **Use existing** option.)
5. Resources comprise the region and the network. On the **Region** page, select a region.
6. On the **Network** page:
   • Type a 1–64 character resources name to help identify the region and network combination in Studio. A resource name cannot contain only blank spaces, or non-ASCII or special characters.
   • Select a virtual network and resource group pair. (Since you can have more than one virtual network with the same name, pairing the network name with the resource group provides unique combinations.) If you selected a region on the previous page that does not have any virtual networks, you need to return to that page and select a region that has virtual networks.
7. Complete the wizard.

**Create a machine catalog using an Azure Resource Manager master image**

This information is a supplement to the guidance in *Create Machine Catalogs*.

A master image is the template that is used to create the VMs in a Machine Catalog. Before creating the machine catalog, create a master image in Azure Resource Manager. For general information about master images, see the *Create Machine Catalogs* article.

In the machine catalog creation wizard:

- The **Operating System** and **Machine Management** pages do not contain Azure-specific information. Follow the guidance in the Create Machine Catalogs article.
- On the **Master Image** page, select a resource group and then navigate (drill down) through the
containers to the Azure VHD you want to use as the master image. The VHD must have a Citrix VDA installed on it. If the VHD is attached to a VM, the VM must be stopped.

- The **Storage and License Types** page appears only when using an Azure Resource Manager master image.

Select a storage type: standard or premium. The storage type affects which machine sizes are offered on the Virtual Machines page of the wizard. Both storage types make multiple synchronous copies of your data within a single data center. For details about Azure storage types and storage replication, see the following:


HUB reduces the cost of running VMs in Azure to the base compute rate, since it waives the price of more Windows Server licenses from the Azure gallery. You need to bring your on-premises Windows Servers images to Azure to use HUB. Azure gallery images are not supported. On-premises Windows Client licenses are currently not supported.

To check if the provisioned VMs are successfully utilizing HUB, run the PowerShell command: `Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM` and check that the license type is **Windows_Server**. More instructions are available at [https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-hybrid-use-benefit-licensing/](https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-hybrid-use-benefit-licensing/).

Azure Managed Disks are used for VMs in the catalog by default. If you want to use regular storage accounts instead, enable the check box at the bottom of the page.

- On the **Virtual Machines** page, indicate how many VMs you want to create; you must specify at least one. Select a machine size. After you create a Machine Catalog, you cannot change the machine size. If you later want a different size, delete the catalog and then create a catalog that uses the same master image and specifies the desired machine size.

Virtual machine names cannot contain non-ASCII or special characters.

- (When using MCS) On the **Resource Groups** page, choose whether to create resource groups or use existing groups.
  - If you choose to create resource groups, click **Next**.
  - If you choose to use existing resource groups, select groups from the **Available Provisioning Resource Groups** list. **Remember**: Select enough groups to accommodate the machines you’re creating in the catalog. Studio displays a message if you choose too few.
You might want to select more than the minimum required if you plan to add more VMs to the catalog later. You can’t add more resource groups to a catalog after the catalog is created.

For more information, see the Azure resource groups section later in this article.

- The Network Cards, Computer Accounts, and Summary pages do not contain Azure-specific information. Follow the guidance in the Create Machine Catalogs article.

Complete the wizard.

Azure resource groups

Azure provisioning resource groups provide a way to provision the VMs that provide applications and desktops to users. You can add existing empty Azure resource groups when you create an MCS machine catalog in Studio, or have new resource groups created for you.

For information about Azure resource groups, see Azure Resource Manager Overview.

Requirements

- Each resource group can hold up to 240 VMs. There must be sufficient available empty resource groups in the region where you’re creating the catalog. If you want to use existing resource groups when you create a machine catalog, you must select enough available groups to accommodate the number of machines that created in the catalog. For example, if you specify 500 machines in the catalog creation wizard, select at least three available provisioning resource groups.

You cannot add resource groups to a machine catalog after the catalog is created. So, consider adding enough resource groups to accommodate machines you might add to the catalog later.

- Create empty resource groups in the same region as your host connection.

- If you want the Citrix Virtual Apps and Desktops service to create resource groups for each MCS catalog, the Azure service principal associated with the host connection must have permission to create and delete resource groups. If you want the Citrix Virtual Apps and Desktops service to use existing empty resource groups, the Azure service principal associated with the host connection must have Contributor permission on those empty resource groups.

- When you create a host connection in Studio using the Create new option, the created service principal has subscription scope contribute permissions. Alternatively, you can use the Use existing option to create the connection, and provide the details of an existing subscription scope service principal. If you use the Create new option and create the Service Principal in Studio, it has the needed permissions to create and delete new resource groups or provision into existing empty resource groups.
• Narrow scope service principals must be created using PowerShell. Also, when using a narrow scope service principal, you must use PowerShell or the Azure portal to create empty resource groups for each catalog where MCS provisions VMs. For instructions, see the blog post https://www.citrix.com/blogs/2016/11/09/azure-role-based-access-control-in-xenapp-xendesktop/.

If you are using narrow scope service principal for the host connection and don’t see your master image resource group on the Master Image page of the catalog creation wizard, it is probably because the narrow scope service principal you are using doesn’t have the permission “Microsoft.Resources/subscriptions/resourceGroups/read” to list the master image resource group. Close the wizard, update the service principal with the permission (see the blog post for instructions), and then restart the wizard. (The update in Azure can take up to 10 minutes to appear in Studio.)

Configure resource groups for a machine catalog in Studio

The Resource Groups page in the catalog creation wizard allows you to choose whether to create resource groups or use existing groups. See Create a machine catalog using an Azure Resource Manager master image.

What happens to resource groups when you delete a machine catalog. If you let the Citrix Virtual Apps and Desktops service create resource groups when you create the machine catalog, and then later delete the catalog, those resource groups, and other resources in those resource groups are also deleted.

If you use existing resource groups when you create the machine catalog, and then later delete the catalog, all resources in those resource groups are deleted, but the resource groups are not deleted.

Considerations, limitations, and troubleshooting

When you use existing resource groups, the list of available resource groups on the Resource Groups page in the catalog creation wizard does not auto-refresh. So, if you have that wizard page open and create or add permissions to resource groups in Azure, the changes are not reflected in the wizard’s list. To see the latest changes, go back to the Machine Management page in the wizard and reselect the resources associated with the host connection. Or, close and restart the wizard. It can take up to 10 minutes for changes made in Azure to appear in Studio.

Use a resource group in only one machine catalog. However, a single resource group in one machine catalog is not enforced. For example, you select 10 resource groups when creating a catalog, but create only one machine in the catalog. Nine of the selected resource groups remain empty after the catalog is created. You might intend to use them to expand your capacity in the future, so they remain associated with that catalog. You can’t add resource groups to a catalog after the catalog is created, so planning for future growth is sound practice. However, if another catalog is created, those nine
resource groups appear in the available list. Citrix Virtual Apps and Desktops does not currently keep track of which resource groups are allocated to which catalogs. It's up to you to monitor that.

If your connection uses a service principal that can access empty resource groups in various regions, they appear in the available list. Be sure to choose resource groups in the same region where you’re creating the machine catalog.

Troubleshooting

Resource groups don’t appear in the list on the Resource Groups page of the catalog creation wizard. The service principal must have appropriate permissions applied to the resource groups you want to appear in the list. See Requirements.

When adding machines to a previously created machine catalog, not all machines are provisioned. After creating a catalog and adding more machines to the catalog, do not exceed the machine capacity of the resource groups originally selected for the catalog (240 per group). You cannot add resource groups after the catalog is created. If you attempt to add more machines than the existing resource groups can accommodate, the provisioning fails.

For example, you create a machine catalog with 300 VMs and 2 resource groups. The resource groups can accommodate up to 480 VMs (240 * 2). If you try to add 200 VMs to the catalog, that exceeds the capacity of the resource groups. 300 current VMs + 200 new VMs = 500, but the resource groups can hold only 480.

More information

- Connections and resources
- Create machine catalogs
- CTX21921: Set up a Microsoft Azure Active Directory account
- CTX219243: Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271: Deploy hybrid cloud using site-to-site VPN

Citrix Hypervisor virtualization environments

May 17, 2019
Create a connection to Citrix Hypervisor

When you create a connection to Citrix Hypervisor (formerly XenServer), you must provide the credentials for a VM Power Admin or higher-level user.

Citrix recommends using HTTPS to secure communications with Citrix Hypervisor. To use HTTPS, you must replace the default SSL certificate installed on Citrix Hypervisor; see CTX128656.

You can configure high availability if it is enabled on the Citrix Hypervisor server. Citrix recommends that you select all servers in the pool (from Edit High Availability) to allow communication with the Citrix Hypervisor server if the pool master fails.

You can select a GPU type and group, or pass through, if the Citrix Hypervisor supports vGPU. The display indicates if the selection has dedicated GPU resources.

When using local storage on one or more Citrix Hypervisor hosts for temporary data storage, make sure that each storage location in the pool has a unique name. (To change a name in XenCenter, right-click the storage and edit the name property.)

Use IntelliCache for Citrix Hypervisor 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 Citrix Hypervisor.

- When installing Citrix Hypervisor, select Enable thin provisioning (Optimized storage for Citrix Virtual Desktops). Citrix does not support mixed pools of servers that have IntelliCache enabled and servers that do not. For more information, see the Citrix Hypervisor documentation.
- In Citrix Virtual Apps and Desktops, IntelliCache is disabled by default. You can change the setting only when creating a Citrix Hypervisor connection; you cannot disable IntelliCache later. When you add a Citrix Hypervisor connection:
  - Select Shared as the storage type.
  - Select the Use IntelliCache check box.
Create a machine catalog using a Citrix Hypervisor connection

GPU-capable machines require a dedicated master image. Those VMs require video card drivers that support GPUs. Configure GPU-capable machines 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 Passthrough or vGPU).
3. Install a supported operating system and enable RDP.
4. Install Citrix VM 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.

More information

- Connections and resources
- Create machine catalogs

Microsoft System Center Virtual Machine Manager virtualization environments

March 6, 2019

Follow this guidance if you use Hyper-V with Microsoft System Center Virtual Machine Manager (VMM) to provide virtual machines.

See System requirements for a list of supported VMM versions.

You can use Machine Creation Services or Citrix Provisioning (formerly Provisioning Services) to provision:

- Generation 1 Desktop or Server OS VMs
- Generation 2 Windows Server 2012 R2, Windows Server 2016, and Windows 10 VMs (with or without Secure Boot)
Install and configure a hypervisor

Install Microsoft Hyper-V server and VMM on your servers.

Verify the following account information:

In Studio, the account you specify when creating a connection must be a VMM administrator or VMM delegated administrator for the relevant Hyper-V machines. If this account has only the delegated administrator role in VMM, the storage data is not listed in Studio during the connection creation process.

Your user account must also be a member of the administrators local security group on each Hyper-V server to support VM lifecycle management (such as VM creation, update, and deletion).

Install the VMM console

Install a System Center Virtual Machine Manager console on each server that contains a Citrix Cloud Connector.

The console version must match the management server version. Although an earlier console can connect to the management server, provisioning VDAs fails if the versions differ.

Create a master VM

- Install a VDA on the master VM, and select the option to optimize the desktop. This improves performance.
- Take a snapshot of the master VM to use as a backup.
- Create virtual desktops.

Create a connection

If you used MCS to provision VMs, in the Studio connection creation wizard:

- Enter the address as a fully qualified domain name of the host server.
- Enter credentials for the administrator account you set up earlier. This account must have permission to create new VMs.
- In the Host Details dialog box, select the cluster or standalone host to use when creating VMs. **Important:** Browse for a 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 \c\ catalogs created with MCS on SMB 3 file shares for VM storage, credentials must meet the following requirements to ensure that calls from the Citrix 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 lifecycle events are performed through the Hyper-V server using the VMM user credentials.

When using VMM 2012 SP1 with Hyper-V on Windows Server 2012: When using SMB as storage, enable the Authentication Credential Security Support Provider (CredSSP) from the Cloud Connector to individual Hyper-V machines. For more information, see CTX 137465.

Using a standard PowerShell V3 remote session, the HCL in the Cloud Connector uses CredSSP to open a connection to the 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. The scripts 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:

```powershell
$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:

```powershell
$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 Cloud Connector, 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 through the Hyper-V machine to the HCL. The following process creates a folder that has only VMM user permissions on the Hyper-V server if it does not exist.

1. The Hyper-V 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.

**More information**

- Connections and resources
- Create machine catalogs

**VMware virtualization environments**

August 29, 2018

Follow this guidance if you use VMware to provide virtual machines.

Install vCenter Server and the appropriate management tools. (No support is provided for vSphere vCenter Linked Mode operation.)

If you plan to use Machine Creation Services (MCS), do not disable the Datastore Browser feature in vCenter Server (described in https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567). If you disable this feature, MCS does not work correctly.
**Required privileges**

Create a VMware user account and one or more VMware roles with a set or all of the privileges listed below. Base the roles’ creation on the specific level of granularly required over the user’s permissions to request the various Citrix Virtual Apps or Citrix Virtual Desktops operations at any time. To grant the user specific permissions at any point, associate them with the respective role, at the DataCenter level at a minimum.

The following tables show the mappings between Citrix Virtual Apps and Desktops operations and the minimum required VMware privileges.

**Add connections and resources**

<table>
<thead>
<tr>
<th>SDK</th>
<th>User interface</th>
</tr>
</thead>
</table>

**Provision machines (Machine Creation Services)**

<table>
<thead>
<tr>
<th>SDK</th>
<th>User interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore.AllocateSpace</td>
<td>Datastore &gt; Allocate space</td>
</tr>
<tr>
<td>Datastore.Browse</td>
<td>Datastore &gt; Browse datastore</td>
</tr>
<tr>
<td>Datastore.FileManagement</td>
<td>Datastore &gt; Low level file operations</td>
</tr>
<tr>
<td>Network.Assign</td>
<td>Network &gt; Assign network</td>
</tr>
<tr>
<td>Resource.AssignVMToPool</td>
<td>Resource &gt; Assign virtual machine to resource pool</td>
</tr>
<tr>
<td>VirtualMachine.Config.AddExistingDisk</td>
<td>Virtual machine &gt; Configuration &gt; Add existing disk</td>
</tr>
<tr>
<td>VirtualMachine.Config.AddNewDisk</td>
<td>Virtual machine &gt; Configuration &gt; Add new disk</td>
</tr>
<tr>
<td>VirtualMachine.Config.RemoveDisk</td>
<td>Virtual machine &gt; Configuration &gt; Remove disk</td>
</tr>
</tbody>
</table>
## SDK vs User Interface

<table>
<thead>
<tr>
<th>SDK</th>
<th>User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualMachine.Inventory.CreateFromExisting</td>
<td>Virtual machine &gt; Inventory &gt; Create from existing</td>
</tr>
<tr>
<td>VirtualMachine.Inventory.Create</td>
<td>Virtual machine &gt; Inventory &gt; Create new</td>
</tr>
<tr>
<td>VirtualMachine.Inventory.Delete</td>
<td>Virtual machine &gt; Inventory &gt; Remove</td>
</tr>
<tr>
<td>VirtualMachine.Provisioning.Clone</td>
<td>Virtual machine &gt; Provisioning &gt; Clone virtual machine</td>
</tr>
<tr>
<td>VirtualMachine.State.CreateSnapshot</td>
<td>vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine &gt; State &gt; Create snapshot; vSphere 5.5: Virtual machine &gt; Snapshot management &gt; Create snapshot</td>
</tr>
</tbody>
</table>

If you want the VMs you create to be tagged, add the following permissions for the user account.

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.

### Global Custom Fields

<table>
<thead>
<tr>
<th>SDK</th>
<th>User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global.ManageCustomFields</td>
<td>Global &gt; Manage custom attributes</td>
</tr>
<tr>
<td>Global.SetCustomField</td>
<td>Global &gt; Set custom attribute</td>
</tr>
</tbody>
</table>

### Provision machines (Citrix Provisioning)

All privileges from **Provision machines (Machine Creation Services)** and the following.

<table>
<thead>
<tr>
<th>SDK</th>
<th>User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualMachine.Config.AddRemoveDevice</td>
<td>Virtual machine &gt; Configuration &gt; Add or remove device</td>
</tr>
<tr>
<td>VirtualMachine.Config.CPUCount</td>
<td>Virtual machine &gt; Configuration &gt; Change CPU Count</td>
</tr>
<tr>
<td>VirtualMachine.Config.Memory</td>
<td>Virtual machine &gt; Configuration &gt; Memory</td>
</tr>
<tr>
<td>VirtualMachine.Config.Settings</td>
<td>Virtual machine &gt; Configuration &gt; Settings</td>
</tr>
<tr>
<td>VirtualMachine.Provisioning.CloneTemplate</td>
<td>Virtual machine &gt; Provisioning &gt; Clone template</td>
</tr>
</tbody>
</table>
## Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>SDK</th>
<th>User interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualMachine.Provisioning.DeployTemplate</td>
<td>Virtual machine &gt; Provisioning &gt; Deploy template</td>
</tr>
</tbody>
</table>

### Power management

<table>
<thead>
<tr>
<th>SDK</th>
<th>User interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualMachine.Interact.Reset</td>
<td>Virtual machine &gt; Interaction &gt; Reset</td>
</tr>
</tbody>
</table>

### Image update and rollback

<table>
<thead>
<tr>
<th>SDK</th>
<th>User interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore.AllocateSpace</td>
<td>Datastore &gt; Allocate space</td>
</tr>
<tr>
<td>Datastore.Browse</td>
<td>Datastore &gt; Browse datastore</td>
</tr>
<tr>
<td>Datastore.FileManagement</td>
<td>Datastore &gt; Low level file operations</td>
</tr>
<tr>
<td>Network.Assign</td>
<td>Network &gt; Assign network</td>
</tr>
<tr>
<td>Resource.AssignVMTToPool</td>
<td>Resource &gt; Assign virtual machine to resource pool</td>
</tr>
<tr>
<td>VirtualMachine.Config.AddExistingDisk</td>
<td>Virtual machine &gt; Configuration &gt; Add existing disk</td>
</tr>
<tr>
<td>VirtualMachine.Config.AddNewDisk</td>
<td>Virtual machine &gt; Configuration &gt; Add new disk</td>
</tr>
<tr>
<td>VirtualMachine.Config.RemoveDisk</td>
<td>Virtual machine &gt; Configuration &gt; Remove disk</td>
</tr>
<tr>
<td>VirtualMachine.Interact.Reset</td>
<td>Virtual machine &gt; Interaction &gt; Reset</td>
</tr>
</tbody>
</table>
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 Cloud Connector.

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 three methods:
   
   **From the vCenter server:**
   
   a) Copy the file rui.crt from the vCenter server to a location accessible on your Cloud Connectors.
b) On the Cloud Connector, 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.

a) Open your web browser and make a secure web connection to the vCenter server (for example https://server1.domain1.com).
b) Accept the security warnings.
c) Click on the address bar displaying the certificate error.
d) View the certificate and click the Details tab.
e) Select **Copy to file and export in .CER format**, providing a name when prompted to do so.
f) Save the exported certificate.
g) Navigate to the location of the exported certificate and open the .CER file.

**Import directly from Internet Explorer running as an administrator:**

a) Open your web browser and make a secure web connection to the vCenter server (for example https://server1.domain1.com).
b) Accept the security warnings.
c) Click on the address bar displaying the certificate error.
d) View the certificate.

3. Import the certificate into the certificate store on each Cloud Connector.

a) Click **Install certificate**, select **Local Machine**, and then click **Next**.
b) Select **Place all certificates in the following store**, and then click **Browse**. On a later supported version: Select **Trusted People** and then click **OK**. Click **Next** and 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 in a machine catalog. On your hypervisor:

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.
Create a connection

In the connection creation wizard:

- Select the VMware connection type.
- Specify the address of the access point for the vCenter SDK.
- Specify the credentials for a VMware user account you set up earlier that has permissions to create new VMs. Specify the username in the form domain/username.

VMware SSL thumbprint

The VMware SSL thumbprint feature addresses a frequently-reported error when creating a host connection to a VMware vSphere hypervisor. Previously, administrators had to manually create a trust relationship between the Citrix-managed Delivery Controllers in the Site and the hypervisor’s certificate before creating a connection. The VMware SSL thumbprint feature removes that manual requirement: the untrusted certificate’s thumbprint is stored on the Site database so that the hypervisor can be continuously identified as trusted by Citrix Virtual Apps or Citrix Virtual Desktops, even if not by the Controllers.

When creating a vSphere host connection, a dialog box allows you to view the certificate of the machine you are connecting to. You can then choose whether to trust it.

More information

- Connections and resources
- Create machine catalogs

Amazon Web Services virtualization environments

July 30, 2019

This article walks you through setting up your Amazon Web Services (AWS) account as a resource location you can use with the Citrix Virtual Apps and Desktops service. The resource location includes a basic set of components, ideal for a proof-of-concept or other deployment that does not require resources spread over multiple availability zones. After you complete these tasks, you can install VDAs, provision machines, create machine catalogs, and create Delivery Groups.

When you complete the tasks in this article, your resource location will include the following components:

- A virtual private cloud (VPC) with public and private subnets inside a single availability zone.
Citrix Virtual Apps and Desktops service

- An instance that runs as both an Active Directory domain controller and DNS server, located in the private subnet of the VPC.
- Two domain-joined instances on which the Citrix Cloud Connector is installed, located in the private subnet of the VPC.
- An instance that acts as a bastion host, located in the public subnet of your VPC. This instance is used to initiate RDP connections to the instances in the private subnet for administration purposes. After you finish setting up your resource location, you can shut down this instance so it is no longer readily accessible. When you need to manage other instances in the private subnet, such as VDA instances, you can restart the bastion host instance.

Task overview

**Set up a virtual private cloud (VPC) with public and private subnets.** When you complete this task, AWS deploys a NAT instance with an Elastic IP address in the public subnet, which enables instances in the private subnet to access the Internet. Instances in the public subnet are accessible to inbound public traffic while instances in the private subnet are not.

**Configure security groups.** Security groups act as virtual firewalls that control traffic for the instances in your VPC. You will add rules to your security groups that allow instances in your public subnet to communicate with instances in your private subnet. You will also associate these security groups with each instance in your VPC.

**Create a DHCP options set.** With an Amazon VPC, DHCP and DNS services are provided by default, which affects how you configure DNS on your Active Directory domain controller. Amazon’s DHCP cannot be disabled and Amazon’s DNS can be used only for public DNS resolution, not Active Directory name resolution. To specify the domain and name servers that should be handed to instances via DHCP, you create a new DHCP options set. The set assigns the Active Directory domain suffix and specifies the DNS server for all instances in your VPC. To ensure Host (A) and Reverse Lookup (PTR) records are automatically registered when instances join the domain, you configure the network adapter properties for each instance you add to the private subnet.

**Add a bastion host, domain controller, and Citrix Cloud Connectors to the VPC.** Through the bastion host, you can log on to instances in the private subnet to set up the domain, join instances to the domain, and install the Citrix Cloud Connector.

**Task 1: Set up the VPC**

1. From the AWS management console, click **VPC**.
2. From the VPC Dashboard, click **Start VPC Wizard**.
3. Select **VPC with Public and Private Subnets** and then click **Select**.
4. Enter a VPC name and change the IP CIDRE block and Public and Private subnet IP ranges, if necessary.
5. If a NAT gateway is selected, click **Use a NAT Instance instead**.
6. For the NAT instance, specify the instance type and the key pair you want to use. The key pair enables you to securely connect to the instance at a later time.
7. In Enable DNS hostnames, leave **Yes** selected.
8. Click **Create VPC**. AWS creates the public and private subnets, Internet gateway, route tables, and default security group. Also, a NAT instance is created and assigned an Elastic IP address.

**Task 2: Configure security groups**

This task creates and configures the following security groups for your VPC:

- A security group for the NAT instance.
- A public security group, with which instances in your Public subnet will be associated.
- A private security group, with which instances in your Private subnet will be associated.

To create the security groups

1. From the VPC Dashboard, click **Security Groups**.
2. Create a security group for the NAT instance: Click **Create Security Group** and enter a name tag and description for the group. In VPC, select the VPC you created earlier. Click **Yes, Create**.
3. Repeat Step 2 to create a public security group and a private security group.

**Configure the NAT security group**

1. From the security group list, select the NAT security group.
2. Click the **Inbound Rules** tab and click **Edit** to create the following rules:

<table>
<thead>
<tr>
<th>Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL Traffic</td>
<td>Select the Private security group.</td>
</tr>
<tr>
<td>22 (SSH)</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

3. When finished, click **Save**.

**Configure the Public security group**

1. From the security group list, select the Public security group.
2. Click the **Inbound Rules** tab and click Edit to create the following rules:
Configure the private security group

1. From the security group list, select the Private security group.
2. Click the inbound Rules tab and click Edit to create the following rules:

<table>
<thead>
<tr>
<th>Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL Traffic</td>
<td>Select the NAT security group.</td>
</tr>
<tr>
<td>ALL Traffic</td>
<td>Select the Private security group.</td>
</tr>
<tr>
<td>ALL Traffic</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>ICMP</td>
<td></td>
</tr>
<tr>
<td>22 (SSH)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>80 (HTTP)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>443 (HTTPS)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>1494 (ICA/HDX)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>2598 (Session Reliability)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>3389 (RDP)</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

5. When finished, click Save.

Configure the public security group

1. From the security group list, select the Public security group.
2. Click the inbound Rules tab and click Edit to create the following rules:

<table>
<thead>
<tr>
<th>Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL Traffic</td>
<td>Select the NAT security group.</td>
</tr>
<tr>
<td>ALL Traffic</td>
<td>Select the Private security group.</td>
</tr>
<tr>
<td>ALL Traffic</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>ICMP</td>
<td></td>
</tr>
<tr>
<td>22 (SSH)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>80 (HTTP)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>443 (HTTPS)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>1494 (ICA/HDX)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>2598 (Session Reliability)</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>
| 3389 (RDP)     | 0.0.0.0/0                                   

3. When finished, click Save.

4. Click the Outbound Rules tab and click Edit to create the following rules:

<table>
<thead>
<tr>
<th>Type</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL Traffic</td>
<td>Select the Private security group.</td>
</tr>
<tr>
<td>ALL Traffic</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>ICMP</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

5. When finished, click Save.
<table>
<thead>
<tr>
<th>Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 53 (DNS)</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>UDP 53 (DNS)</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>80 (HTTP)</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>TCP 135</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>TCP 389</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>UDP 389</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>443 (HTTPS)</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>TCP 1494 (ICA/HDX)</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>TCP 2598 (Session Reliability)</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>3389 (RDP)</td>
<td>Select the Public security group.</td>
</tr>
<tr>
<td>TCP 49152-65535</td>
<td>Select the Public security group.</td>
</tr>
</tbody>
</table>

3. When finished, click **Save**.

4. Click the **Outbound Rules** tab and click **Edit** to create the following rules:

<table>
<thead>
<tr>
<th>Type</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL Traffic</td>
<td>Select the Private security group.</td>
</tr>
<tr>
<td>ALL Traffic</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>ICMP</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>UDP 53 (DNS)</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

5. When finished, click **Save**.

**Task 3: Associate the NAT instance with the NAT security group**

1. From the AWS management console, click **EC2**.
2. From the EC2 Dashboard, click **Instances**.
3. Select the NAT instance and then click **Actions > Networking > Change Security Groups**.
4. Clear the default security group check box.
5. Select the NAT security group you created earlier and then click **Assign Security Groups**.
Task 4: Launch instances

The following steps create four EC2 instances and decrypt the default Administrator password that Amazon generates.

1. From the AWS management console, click EC2.
2. From the EC2 Dashboard, click Launch Instance.
3. Select a Windows Server machine image and instance type.
4. On the Configure Instance Details page, enter a name for the instance and select the VPC you set up earlier.
5. In Subnet, make the following selections for each instance:
   - Bastion host: Select the Public subnet.
   - Domain controller and Connectors: Select the Private subnet.
6. In Auto-assign Public IP address, make the following selections for each instance:
   - Bastion host: Select Enable.
   - Domain controller and Connectors: Select Use default setting or Disable.
7. In Network Interfaces, enter a primary IP address within the IP range of your private subnet for the domain controller and Cloud Connector instances.
8. On the Add Storage page, modify the disk size, if necessary.
9. On the Tag Instance page, enter a friendly name for each instance.
10. On the Configure Security Groups page, select Select an existing security group and then make the following selections for each instance:
    - Bastion host: Select the Public security group.
    - Domain controller and Cloud Connectors: Select the Private security group.
11. Review your selections and then click Launch.
12. Create a new key pair or select an existing one. If you create a new key pair, download your private key (.pem) file and keep it in safe place. You will need to supply your private key when you acquire the default Administrator password for the instance.
13. Click Launch Instances. Click View Instances to display a list of your instances. Wait until the newly-launched instance has passed all status checks before accessing it.
14. Acquire the default Administrator password for each instance:
   a) From the instance list, select the instance and then click Connect.
   b) Click Get Password and supply your private key (.pem) file when prompted.
   c) Click Decrypt Password. AWS displays the default password.
15. Repeat Steps 2-14 until you have created four instances: a bastion host instance in your public subnet and three instances in your private subnet that for use as a domain controller and two Cloud Connectors.

**Task 5: Create a DHCP options set**

1. From the VPC Dashboard, click **DHCP Options Sets**.

2. Enter the following information:
   - Name tag: Enter a friendly name for the set.
   - Domain name: Enter the fully qualified domain name you will use when you configure the domain controller instance.
   - Domain name servers: Enter the private IP address you assigned to the domain controller instance and the string `AmazonProvidedDNS`, separated by commas.
   - NTP servers: Leave this field blank.
   - NetBIOS name servers: Enter the private IP address of the domain controller instance.
   - NetBIOS node type: Enter 2.

3. Click **Yes, Create**.

4. Associate the new set with your VPC:
   a) From the VPC Dashboard, click **Your VPCs** and then select the VPC you set up earlier.
   b) Click **Actions > Edit DHCP Options Set**.
   c) When prompted, select the new set you created and then click **Save**.

**Task 6: Configure the instances**

1. Using an RDP client, connect to the public IP address of the bastion host instance. When prompted, enter the credentials for the Administrator account.

2. From the bastion host instance, launch Remote Desktop Connection and connect to the private IP address of the instance you want to configure. When prompted, enter the Administrator credentials for the instance.

3. For all instances in the private subnet, configure the DNS settings:
   a) Click **Start > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**. Double-click the network connection displayed.
   b) Click **Properties**, select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
   c) Click **Advanced** and then click the **DNS** tab. Ensure the following settings are enabled and click **OK**.
Citrix Virtual Apps and Desktops service

• Register this connection’s addresses in DNS
• Use this connection’s DNS suffix in DNS registration

4. To configure the domain controller:

   a) Using Server Manager, add the Active Directory Domain Services role with all default features.
   b) Promote the instance to a domain controller. During promotion, enable DNS and use the domain name you specified when you created the new DHCP options set. Restart the instance when prompted.

5. To configure the first Cloud Connector:

   a) Join the instance to the domain and restart when prompted. From the bastion host instance, reconnect to the instance using RDP.
   b) Sign in to Citrix Cloud. Select Resource Locations from the upper left menu.
   c) Download the Cloud Connector.
   d) When prompted, run the cwccconnector.exe file and supply your Citrix Cloud credentials. Follow the wizard.
   e) When finished, click Refresh to display the Resource Locations page. When the Cloud Connector is registered, the instance appears on the page.

6. Repeat Step 5 to configure the second Cloud Connector.

Create a connection

When you create a connection using Studio:

• You must provide the API key and secret key values. You can export the key file containing those values from AWS and then import them. You must also provide the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials.
• 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, Citrix Virtual Apps and Desktops management cannot use the file to populate the API key and secret key fields. Ensure that you are using AWS IAM credentials files.

More information

• Connections and resources
• Create machine catalogs
Nutanix virtualization environments

August 29, 2018

Follow this guidance when using Nutanix Acropolis to provide virtual machines in your Citrix Virtual Apps or Citrix Virtual Desktops deployment. The setup process includes the following tasks:

- Install and register the Nutanix plugin in your Citrix Virtual Apps or Citrix Virtual Desktops environment.
- Create a connection to the Nutanix Acropolis hypervisor.
- Create a machine catalog that uses a snapshot of a master image you created on the Nutanix hypervisor.

For more information, see the Nutanix Acropolis MCS Plugin Installation Guide, available at the Nutanix Support Portal.

Install and register the Nutanix plugin

Complete the following procedure to install and register the Nutanix plugin on the Cloud Connectors. You will then be able to use the Manage functions in Citrix Cloud to create a connection to the Nutanix hypervisor and then create a machine catalog that uses a snapshot of a master image you created in the Nutanix environment.

1. Obtain the Nutanix plugin from Nutanix, and install it on the Cloud Connectors.
2. Verify that a Nutanix Acropolis folder has been created in C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0.
3. Run C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe –PluginsRoot “C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0”.
5. Run the following PowerShell cmdlets to verify that the Nutanix Acropolis plugin is registered:
   
   Add-PSSnapin Citrix
   Get-HypHypervisorPlugin

Create a connection to Nutanix

In the Add Connection and Resources wizard, select the Nutanix connection type on the Connection page, and then specify the hypervisor address and credentials, plus a name for the connection. On the Network page, select a network for the hosting unit.
Create a machine catalog using a Nutanix snapshot

This information is a supplement to the guidance in Create machine catalogs. It describes only the fields that are unique to Nutanix.

The snapshot you select is the template that will be used to create the VMs in the catalog. Before creating the catalog, create images and snapshots in Nutanix. See the Nutanix documentation for guidance.

In the catalog creation wizard:

- The Operating System and Machine Management pages do not contain Nutanix-specific information.
- On the Container page, which is unique to Nutanix, select the container where the VMs’ disks will be placed.
- On the Master Image page, select the image snapshot. Acropolis snapshot names must be prefixed with “XD_” to be used in Citrix Virtual Apps and Desktops. Use the Acropolis console to rename your snapshots, if needed. If you rename snapshots, restart the catalog creation wizard to see a refreshed list.
- On the Virtual Machines page, indicate the number of virtual CPUs and the number of cores per vCPU.
- The Network Cards, Computer Accounts, and Summary pages do not contain Nutanix-specific information.

More information

- Connections and resources
- Create machine catalogs

Google Cloud Platform virtualization environments

October 8, 2019

The Citrix Virtual Apps and Desktops service lets you provision and manage machines on Google Cloud Platform (GCP). This article walks you through using Machine Creation Services (MCS) to provision virtual machines in your Citrix Virtual Apps or Citrix Virtual Desktops service deployment.
Citrix Virtual Apps and Desktops service

Requirements

- Citrix Cloud account. The feature described in this article is available only in Citrix Cloud.
- Citrix Virtual Apps and Desktops service subscription. For details, see Get started.
- A GCP project. The project stores all compute resources associated with the machine catalog. It can be an existing project or a new one.
- Enable four APIs in your Google Cloud project. For details, see Enable Google Cloud APIs.
- GCP service account. The service account authenticates to Google Cloud to enable access to the project. For details, see Configure the Google Cloud service account.

Enable Google Cloud APIs

To use the Google Cloud functionality through Citrix Studio, enable these APIs in your Google Cloud project:

- Compute Engine API
- Cloud Resource Manager API
- Identity and Access Management (IAM) API
- Cloud Build API

From the GCP main screen, complete these steps:

1. In the upper left menu, select APIs and Services > Dashboard.
2. On the Dashboard screen, ensure that Compute Engine API is enabled. If not, follow these steps:

   a) Navigate to APIs and Services > Library.
b) In the search box, type *Compute Engine*.

c) From the search results, click Compute Engine API.

d) On the Compute Engine API screen, click Enable.

3. Enable Cloud Resource Manager API.

   a) Navigate to APIs and Services > Library.
   
   b) In the search box, type *Cloud Resource Manager*.
   
   c) From the search results, click Cloud Resource Manager API.
   
   d) On the Cloud Resource Manager API screen, click Enable. The API’s status appears.

4. Similarly, enable Identity and Access Management (IAM) API and Cloud Build API.

**Configure the Google Cloud service account**

A Google Cloud service account lets you create and manage resources inside GCP projects. A Google Cloud service account is required to provision and manage machines as described in this article. The Google Cloud account authenticates to Citrix Cloud using a key generated by Google Cloud. Each account (personal or service) contains various roles defining the management of the project.

We recommend that you create a new service account. To do so, follow these steps:

1. In the Google cloud console, navigate to IAM & admin > Service accounts.
2. On the Service accounts page, click **CREATE SERVICEACCOUNT**.

3. On the **Create service account** page, type the required information and then click **CREATE**.

   **Tip:**
   - You can click **CANCEL** to save and exit the Service account details page without completing the **Grant this service account access to project** and the **Grant users access to this service account** pages. We recommend that you complete the remaining two pages later.

When creating a service account, there is an option to create a key for the account. You need this key when creating a connection in Citrix Studio. The key is contained in a credential file (.json). The file is automatically downloaded and saved to the “Downloads” folder after you create the key. When you create the key, make sure to set the key type to JSON. Otherwise, Studio cannot parse it.

   **Tip:**
   Create keys using the **Service accounts** page in the GCP console. We recommend that you change keys regularly for security purposes. You can provide new keys to the Citrix Virtual Apps and Desktops application by editing an existing GCP connection.

Also, you need to grant your service account the necessary permissions to access your GCP project. To do so, follow these steps:

1. In the Google Cloud console, navigate to **IAM & admin > IAM**.

2. On the IAM page, locate the service account you created and then click the pencil icon to edit the service account.

3. On the **Edit permissions** page, click **ADD ANOTHER ROLE** to add the following roles to your service account one by one and then click **SAVE**.
   - Compute Admin
   - Storage Admin
   - Cloud Build Editor
   - Service Account User
   - Cloud Datastore User

4. Update the roles assigned to your project’s Cloud Build service account.
   a) In the Google Cloud console, navigate to **IAM & admin > IAM**.
   b) On the IAM page, locate the Cloud Build service account and then click the pencil icon to edit the service account. You can identify the Cloud Build service account by its user name, which is in this format: `<your_gcp_project_ID_number>@cloudbuild.gserviceaccount.com`.  

© 1999-2019 Citrix Systems, Inc. All rights reserved.
c) On the Edit permissions page, click ADD ANOTHER ROLE to add the following roles to your Cloud Build service account one by one and then click SAVE.
   - Cloud Build Service Account
   - Compute Instance Admin
   - Service Account User

Add a connection

In Citrix Studio, follow the guidance in Create a connection and resources. The following description guides you through setting up a hosting connection in Citrix Studio:

1. On the Manage tab, navigate to Configuration > Hosting in the Studio navigation pane.
2. In the Actions pane, click Add Connection and Resources.
3. On the Connection page, select Create a new Connection and Studio tools and then click Next.
   - Connection type. Select Google Cloud Platform from the menu.
   - Service account key. Import the key contained in your Google credential file (.json). To do so, locate your credential file, open the file with Notepad (or any text editor), and then copy the content. After that, return to the Connection page, click Import key, paste the content, and then click OK.
   - Service account ID. The field automatically populates with the information from the imported key.
   - Connection name. Type a name for the connection*.
4. On the Region page, select a project name from the menu, select a region containing the resources you want to use, and then click Next.
5. On the Network page, type a name for the resources*, select a virtual network from the menu, select a subset, and then click Next. The resource name helps identify the region and network combination in Studio.

| * Note: |
| The resource name can contain 1–64 characters, and cannot contain only blank spaces or the characters `\ / ; : # * ? = < > | [ ] { } "' ( )`. |

6. On the Summary page, confirm the information and then click Finish to exit the Add Connection and Resources window.

After creating the connection and resources, Studio lists the connection and resources you created. You might want to configure the connection. To do so, select the connection and then click the applicable option in the Actions pane.
Similarly, you can choose to delete, rename, or test the resources created under the connection. To do so, select the resource under the connection and then click the applicable option in the Actions pane.

**Prepare a master VM instance and a persistent disk**

Tip:

Persistent disk is the GCP term for virtual disk.

To prepare your master VM instance, create and configure a VM instance with properties that match the configuration you want for the cloned VDA instances in your planned machine catalog. The configuration doesn’t apply only to the instance size and type. It also includes instance attributes such as metadata, tags, GPU assignments, network tags, and service account properties.

As part of the mastering process, MCS uses your master VM instance to create the GCP “instance template.” The instance template is then used to create the cloned VDA instances that make up the machine catalog. Cloned instances inherit the properties (except the VPC, subnet, and persistent disk properties) of the master VM instance from which the instance template was created.

After configuring the properties of the master VM instance to your specifics, start the instance and then prepare the persistent disk for the instance.

We recommend that you manually create a snapshot of the disk. Doing so lets you use a meaningful naming convention to track versions, gives you more options to manage earlier versions of your master image, and saves time for machine catalog creation. If you don’t create your own snapshot, MCS creates one for you. You can use it to create the custom image in your GCP image library.

**Create a machine catalog**

Note:

Create your resources before you create a machine catalog.

In Citrix Studio, follow the guidance in Create machine catalogs. The following description is unique to Google Cloud Platform catalogs.

1. On the Manage tab, select Machine Catalogs in the Studio navigation pane.

2. In the Actions pane, click Create Machine Catalog.

3. On the Operating System page, select Multi-session OS and then click Next.
   - The Citrix Virtual Apps and Desktops service also supports single-session OS.
4. On the Machine Management page, select the Machines that are power managed and the Citrix Machine Creation Services options and then click Next. If there are multiple resources, you need to select one from the menu.

5. On the Master Image page, select a VM and the minimum functional level for the catalog and then click Next.

6. On the Virtual Machines page, specify how many VMs you want to create, view the detailed specification of the VMs, and then click Next.

7. On the Computer Accounts page, select an Active Directory account and then click Next.
   - If you select Create new Active Directory accounts, select a domain and then type a name for the account naming scheme.
   - If you select Use existing Active Directory accounts, click Browse to navigate to the existing Active Directory computer accounts for the selected machines.

8. On the Domain Credentials page, click Enter credentials, type the user name and password, click OK, and then click Next.
   - The credential you type must have permissions to perform Active Directory account operations.

9. On the Scopes page, select scopes for the machine catalog and then click Next.
   - You can select optional scopes or click custom scope to customize scopes as needed.

10. On the Summary page, confirm the information, specify a name for the catalog, and then click Finish.

    Note:
    The catalog name can contain 1–39 characters, and cannot contain only blank spaces or the characters \ / ; : ## . * ? = < > | [ ] { } ” ’ ( ) .

It might take a long time for the machine catalog creation to complete. After the catalog creation completes, Studio lists the catalog you created.

Add machines to a catalog

To add machines to a catalog, follow these steps:

1. In the Studio navigation pane, select Machine Catalogs.
2. Select the machine catalog to which you want to add machines.
3. In the Actions pane, click Add Machines.
4. On the Virtual Machines page, specify the number of machines you want to add and then click Next.
5. On the **Computer Accounts** page, select an Active Directory account and then click **Next**.

6. On the **Domain Credentials** page, click **Enter credentials**, type the user name and password, click **OK**, and then click **Next**.

7. On the **Summary** page, confirm the information and then click **Finish**.

**Update machines**

This feature can be useful in cases where you want to update your master image or the minimum functional level.

To update machines, follow these steps:

1. In the Studio navigation pane, select **Machine Catalogs**.
2. Select the machine catalog that contains machines you want to update.
3. In the **Actions** pane, click **Update Machines**.
4. On the **Master Image** page, select a VM and the minimum functional level for the catalog and then click **Next**.
5. On the **Rollout Strategy** page, specify when you want to update the machines and then click **Next**.
6. On the **Summary** page, confirm the information and then click **Finish**.

To roll back a machine update, follow these steps:

**Important:**

Do not rename, delete, or move master images. Otherwise you cannot roll back the update.

1. In the Studio navigation pane, select **Machine Catalogs**.
2. Select the machine catalog where you want to roll back the machine update.
3. In the **Actions** pane, click **Rollback Machine Update**.
4. On the **Overview** page, confirm the information and then click **Next**.
5. On the **Rollout Strategy** page, configure the rollout strategy and then click **Next**.
6. On the **Summary** page, confirm the information and then click **Finish**.

**Power management**

The Citrix Virtual Apps and Desktops service lets you power manage GCP machines. Use the Search node in the navigation pane to locate the machine you want to power manage. The following power actions are available:
Citrix Virtual Apps and Desktops service

- Delete
- Start
- Restart
- Force Restart
- Shut Down
- Force Shutdown
- Add to Delivery Group
- Manage Tags
- Turn on Maintenance Mode

You can also power manage the GCP machines by using Autoscale. To do so, add the GCP machines to a Delivery Group and then enable Autoscale for that Delivery Group. For more information about Autoscale, see Autoscale.

**Import manually created GCP machines**

You can create a connection to GCP and then create a catalog containing GCP machines. Then, you can manually power cycle GCP machines through Citrix Virtual Apps and Desktops service. With this feature, you can:

- Import manually created GCP multi-session OS machines into a Citrix Virtual Apps and Desktops machine catalog.
- Remove manually created GCP multi-session OS machines from a Citrix Virtual Apps and Desktops catalog.
- Use existing Citrix Virtual Apps and Desktops power management capabilities to power manage GCP Windows Server machines. For example, set a restart schedule for those machines.

This functionality does not require changes to an existing Citrix Virtual Apps and Desktops provisioning workflow, nor the removal of any existing feature. We recommend that you use MCS to provision machines in Studio instead of importing manually created GCP machines.

**More information**

- Connections and resources
- Create machine catalogs

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Install Cloud Connectors

September 5, 2019

Citrix Cloud Connectors bridge the gap between the Citrix-managed services and customer-managed components. The Cloud Connector is a group of services from Citrix Cloud that allow communication between the VDAs, customer-managed StoreFront, and the cloud-based Delivery Controller. You can install Cloud Connectors interactively or from the command line.

After you finish installing the first Cloud Connector, repeat the steps for the second Cloud Connector in the resource location. You should have a minimum of two Cloud Connectors in each resource location.

After installation, ensure that the servers containing Cloud Connectors are powered on at all times for proper operation. Do not move a machine containing a Cloud Connector to a different domain.

Size and scale considerations

When evaluating the Citrix Virtual Apps and Desktops service for sizing and scalability, consider all of the components. Research and test the configuration of the Cloud Connectors and the customer-managed StoreFront for your specific requirements. Undersizing the machines can impact system performance negatively.

The following articles contain size and scale testing information. They provide details of the tested maximum capacities, plus best practice recommendations for Cloud Connector machine configuration.

- Scale and size considerations for Cloud Connectors
- Scale and size considerations for Local Host Cache

Prepare machines

Provision two Windows Server 2012 R2 or Windows Server 2016 machines.

Each machine hosting the Cloud Connector must meet the following requirements:

- Microsoft .NET Framework 4.7.2 or later installed.
- Joined to an Active Directory domain that contains the resources and users that you will use to create offerings for your users.
- Connected to a network that can contact the resources you will use in your resource location. For more information, see Cloud Connector Proxy and Firewall Configuration.
- Connected to the Internet. For more information, see Internet Connectivity Requirements.
- Server clock is set to the correct UTC time.
Citrix Virtual Apps and Desktops service

- Outbound TCP port 443 is open for communication with Citrix Cloud.

When using Microsoft System Center Virtual Machine Manager to provision machines that deliver apps and desktops (the host), install a VMM console on each server that contains a Citrix Cloud Connector. If you omit this installation, an error message displays: “SCVMM console version 2012 or later is not installed on the following delivery controllers …”

**Install a Cloud Connector interactively**

From the server where you’ll install the Cloud Connector, log on to Citrix Cloud. From the menu in the upper left corner, select **Resource Locations**.

![Resource Locations](image)

Click **Download** and then follow the wizard.

- You are asked for Citrix Cloud administrator credentials. (These are the credentials you used to log on to Citrix Cloud.)
- If you are an administrator for more than one customer, choose the customer for whom you’re installing the Cloud Connector.
- If the customer has more than one resource location, choose the one where you want to install the Cloud Connector.

The installer runs connectivity checks to Citrix Cloud at the beginning and end of the installation.
After you finish installing the first Cloud Connector, repeat the steps for the second Cloud Connector in the resource location. Each resource location should have a minimum of two Cloud Connectors. Citrix recommends downloading a new Cloud Connector from the Citrix Cloud Control Center for each installation. Do not re-use a download to install more than one Cloud Connector.

**Install a Cloud Connector from the command line**

Run the following command:

```bash
```

To display a list of supported parameters, enter: `CWCCConnector /?`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>q</td>
<td>Initiates a silent installation. If omitted, an interactive installation launches.</td>
</tr>
<tr>
<td>ClientId</td>
<td>Required. Secure client ID an administrator can create. Find on the API Access page.</td>
</tr>
<tr>
<td>ClientSecret</td>
<td>Required. Secure client secret available by download after creating a secure client. Find on the API Access page.</td>
</tr>
<tr>
<td>ResourceLocationId</td>
<td>Optional. Find on the Resource Locations page, using the ID button.</td>
</tr>
<tr>
<td>AcceptTermsOfService</td>
<td>Required.</td>
</tr>
</tbody>
</table>

**Installation results**

Exit codes:

- 1603: An unexpected error occurred.
- 2: A prerequisite check failed.
- 0: The installation completed successfully.

Installation logs are stored at:

- `%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup`
Citrix Virtual Apps and Desktops service

- %ProgramData%\Citrix\WorkspaceCloud\InstallLogs

If an installation fails, run `Start /Wait CWConnector.exe /parameter:value` to examine error codes. After the installation completes, run `echo %ErrorLevel%`.

More information

- Citrix Cloud Connector
- Citrix Cloud Connector Technical Details
- Cloud Connector Installation
- Cloud Connector Proxy and Firewall Configuration
- Scale and size considerations for Cloud Connectors
- Scale and size considerations for Local Host Cache

Where to go next

Create a connection

To review the entire configuration process, see Install and configure.

Scale and size considerations for Cloud Connectors

September 30, 2019

When evaluating the Citrix Virtual Apps and Desktops service for sizing and scalability, consider all the components. Research and test the configuration of the Cloud Connectors and the customer-managed StoreFront for your specific requirements. Undersizing the machines can impact system performance negatively. This article provides details of the tested maximum capacities, and best practice recommendations for Cloud Connector machine configuration.

Summary

All results in this summary are based on the findings from a test environment as configured in the detailed sections of this document. Different system configurations may yield different results.

Key results from testing:

- The Citrix Virtual Apps and Desktops service sizing and scalability
  - A set of three 4-vCPU Cloud Connectors is recommended for sites that host no more than 5,000 Workstation VDAs.
This is an N+1 High Availability configuration.

- Starting 20,000 sessions to 100 Server VDAs is 57% faster using customer-managed StoreFront compared to using Citrix-managed StoreFront.
- Provisioning 1,000 VMs takes an average of 140 minutes.

**Citrix Virtual Desktops Essentials**

- Two Cloud Connectors hosted on Azure Standard_A2_v2 VMs are recommended for 1,000 Windows 10 VMs.
- Starting 1,000 sessions to Windows 10 VMs hosted in Azure takes less than 20 minutes.
- Testing found that it takes approximately 44 seconds from when a user logs on to StoreFront until the user receives a functional VDI desktop with default settings.
- Provisioning 1,000 Windows 10 VMs in Azure takes an average of 8 hrs.

**Environment Overview**

- Citrix Cloud manages Cloud Connector services, and the customer manages the machines.
- Session launch testing for Citrix Virtual Desktops Essentials used a NetScaler appliance. All other session launch testing used connections direct to StoreFront.

**Test methodology**

Tests were conducted to add load and to measure the performance of the environment components. The components were monitored by collecting performance data and procedure timing (such as logon time, machine creation time). In some cases, proprietary Citrix simulation tools were used to simulate VDAs and sessions. These tools are designed to exercise Citrix components the same way that traditional VDAs and sessions do, without the same resource requirements to host real sessions and VDAs. We executed the following tests:

- Session logon storm: a test that simulates high-volume logon periods
Citrix Virtual Apps and Desktops service

- VDA registration storm: a test that simulates high-volume VDA registration periods. For example, following an upgrade cycle or outage recovery.
- Machine Creation Service provisioning: a test that measure the time to perform tasks such as copying master images, creating Active Directory accounts, and creating machines.

We used the data gathered from these tests to make recommendations for Cloud Connector sizing. The test execution details follow.

**Session logon storm tests**

Sessions are started at customer-managed and Citrix-managed StoreFront servers independently. 1,000 session, 5,000 session, and 20,000 session tests were run against each environment. We collected StoreFront logon, resource enumeration, ICA file retrieval, and active desktop times. The active desktop time is the time from when the ICA file starts until the resource is fully loaded and ready to use.

For some test scenarios, we used simulation tools to facilitate testing of larger user counts. Simulation tools allow testing using less hardware than is required to run 5,000 or 20,000 real sessions. These simulated sessions go through the normal StoreFront logon, resource enumeration, and ICA file retrieval, but do not start active desktops. Instead, the simulation tool reports to the ICA stack that the session has started. All communication from the broker agent to the Broker Service is consistent with the communication of an actual session. Performance metrics are gathered from the Cloud Connectors.

To determine how the environment responded to session launches, a sustained concurrency of 25 session launches was maintained throughout the duration of the test. The measurements therefore show the results of a system under load throughout the test.

**VDA registration storm tests**

In a VDA registration storm, hundreds or thousands of VDAs are registered all at once to simulate a site recovery. High-volume VDA registration typically happens after the upgrade cycle every two weeks, during a “Monday morning” scenario, or when the system recovers from an outage between customer managed machines and Citrix-managed services. Tests were conducted using 5,000 VDAs and the Cloud Connectors were monitored by gathering performance data during each test. Data included Perfmon counters (CPU, memory, disk utilization) and VDA registration times.

**Machine Creation Service provisioning tests**

Provisioning tests were performed by creating catalogs of varying counts. The times for various tasks (master image copy, AD account creation, and machine creation) were measured to gauge perfor-
mance. We tested catalog size increases in Azure. Both Azure and customer-managed hypervisors underwent 1,000 machine provisioning testing. The testing in Azure was limited to Windows 10 VMs because Windows 10 is the only supported OS for Citrix Virtual Desktops Essentials. The customer-managed hypervisor was tested on Windows 10 and on Windows 2012 R2.

**Test environment**

The test environment configuration included Citrix Cloud Connector, Citrix Virtual Apps and Desktops service and Citrix Virtual Apps and Desktops components. The machine and operating system specifications we used are provided here so you can compare our configuration and test results to your own configuration and requirements.

**Tools used**

An internal testing tool collected performance data and metrics from the machines under test, and drove the session launches. This proprietary tool orchestrates user session launches to the Citrix Virtual Apps and Desktops environment, and provides a central location for collecting response time data and performance metrics. In essence, the test tool administers the tests and collects the results.

**Test configuration – Citrix Virtual Apps and Desktops**

The following is a list of the machine and OS specifications used during Citrix Virtual Apps and Desktops testing.

- **Cloud Connectors:**
  - Scenario One: Two Windows 2012 R2, 2 vCPU, 4 GB memory
  - Scenario Two: Two Windows 2012 R2, 4 vCPU, 4 GB memory
- **StoreFront (customer-managed):** One Windows 2012 R2, 8 vCPU, 8 GB memory
- **Hypervisors:** Eight VMware vSphere ESXi 6.0 Update 1, HP ProLiant BL 460c Gen9, Two Intel E5-2620 CPU, 256 GB Memory
- **Hypervisor Storage:** 2-TB NFS share on NetApp 3250
- **VDA:** Windows 2012 R2 and Windows 10 32-bit Build 1607

**Test configuration – Citrix Virtual Desktops Essentials**

Sessions were started from 100 Windows 2012 R2 client launcher machines. Sessions were authenticated against a Windows Active Directory hosted in Azure. Roaming profiles were stored on a Windows file server in Azure.

- **VDA:** 1,000 Windows 10 64-bit Build 1607, 2 vCPU, 7 GB memory (Standard_D2_v2 instance)
Citrix Virtual Apps and Desktops service

- **Client**: 100 Windows 2012 R2 Servers, 8 vCPU, 8 GB memory
- **Domain Controller**: Two Windows 2012 R2, 4 vCPU, 14 GB memory (Standard_D3_v2 instance)
- **File Server**: One Windows 2012 R2, DS11 instance
- **NetScaler VPX**: One NetScaler 11.0, Standard_D3_v2 instance that has 1,000 Platinum license
- **Cloud Connectors**:
  - **Scenario One**: Two Windows 2012 R2, 2 vCPU, 4 GB memory (Standard_A2_v2 instance)
  - **Scenario Two**: Two Windows 2012 R2, 4 vCPU, 7 GB memory (Standard_A3 instance)
- **StoreFront (customer-managed)**: One Windows 2012 R2, DSv2 instance

**Customer-managed machine considerations**

Customer-managed machines can be in the customer office, data center, or cloud account (such as Azure or AWS). By our definition, customer-managed machine is under the complete customer control. Customer-managed machines include: Cloud Connector, StoreFront servers, RDS servers, VDI machines, and Remote PC Access machines (not covered during testing). For the sake of brevity, we refer to RDS servers, VDI machines, and Remote PC Access machines as VDAsthroughout this report.

**StoreFront servers**

We used an 8-vCPU, 8-GB memory machine as the customer-managed StoreFront server when we tested the Citrix Virtual Apps and Desktops service. For Citrix Virtual Desktops Essentials testing, we used an Azure Standard_DS2_v2 (2 vCPU, 7 GB memory) for the customer-managed StoreFront server. See the StoreFront Planning Guide to size your StoreFront server properly for your environment.

**Cloud Connectors**

We tested customer-managed Cloud Connectors hosted on VMs that had 2-vCPU and 4-GB memory in one scenario, and 4-vCPU and 4-GB memory in another. In Azure, Cloud Connectors were tested on Standard_A2_v2 (2 vCPU, 4 GB memory) and Standard_A3 (4 vCPU, 7 GB memory) instances.

In our testing, Cloud Connectors were deployed in HA sets (**they are not load-balanced**). Although this document focuses on testing environments that have two Cloud Connectors, an N+1 set of three Cloud Connectors is recommended. The rest of this report focuses on the Cloud Connectors and how to size them for best performance.
Test results

VDA registration storm

The VDA Registration Storm test provides data that shows the relationship between Cloud Connector sizing and environment stability. Environment stability is tested during cases of a network outage between the customer-managed location and the Citrix-managed services. VDA registration storms can be triggered when the Delivery Controller and the Site database are upgraded, typically every two weeks.

Cloud Connector CPU sizing comparison 2 vCPU vs. 4 vCPU

- The average usage is similar, but the 2-vCPU machine CPU is under strain during the test and occasional VDA de-registrations are observed.
- The use of 4-vCPU Cloud Connectors for sites that have approximately 5,000 VDAs is recommended for stability.
- The use of 2-vCPU Cloud Connectors is recommended for sites that host 2,500 VDAs.
- Cloud Connectors are a high-availability set and do not load balance.
- One reason we do not recommend the 2-vCPU Cloud Connector for sites that host 5,000 VDAs is the randomness of machine assignment. Because the Cloud Connectors are not load-balanced, you cannot predict the size of the load being funneled to either Cloud Connector. Sometimes, we found more than 60% of the load funneled to one machine.
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Number of VDAs</th>
<th>Cloud Connectors required</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;2,500</td>
<td>2 VMs + 1, each having 2 vCPUs</td>
</tr>
<tr>
<td>&lt;5,000</td>
<td>2 VMs + 1, each having 4 vCPUs</td>
</tr>
</tbody>
</table>

**Cloud Connector HA pair VDA registration storm timing comparison**

<table>
<thead>
<tr>
<th>Cloud Connector size</th>
<th>VDA count</th>
<th>Registration time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 vCPU</td>
<td>5000</td>
<td>11:03</td>
</tr>
<tr>
<td>4 vCPU</td>
<td>5000</td>
<td>5:46</td>
</tr>
</tbody>
</table>

- The Cloud Connectors equipped with 4 vCPUs proved to be more stable during testing.
- VDAs registered faster when Cloud Connectors were equipped with 4 vCPUs.
- VDA re-registrations were observed during testing with the 2-vCPU Cloud Connectors.
  - Re-registrations may occur when registration attempts timeout, or VDA communication heartbeats are delayed.

**Memory usage by component on a Cloud Connector during a 5,000 VDA registration storm**

![Memory Usage by Component](image_url)
Citrix Virtual Apps and Desktops service

- This graph is a detailed view of the memory usage by Citrix components and Microsoft LSASS (Local Security Authority Subsystem Service), during the registration storm test.
- The LSASS process on the Cloud Connectors plays an important part in both registrations and session launches. All Active Directory authentications, made by the Citrix Cloud services, are proxied to the customer-managed Active Directory via the Cloud Connectors.
- Memory usage peaks during the VDA registration period, decreasing after all the VDAs register successfully.
- High memory utilization is observed on Cloud Connectors that have 4 GB of memory.

Session launch (Citrix Virtual Desktops Essentials)

1,000 session launch tests were conducted using the Citrix Virtual Desktops Essentials platform. Testing compared different-sized Cloud Connector instances. We tested the Standard_A2_v2 (2 vCPU, 4 GB memory) and Standard_A3 (4 vCPU, 7 GB memory) instances.

Connector CPU usage with Citrix manage StoreFront during session launch test

- There is low CPU contention during the test. The Standard_A2_v2 instance size was more than able to handle a 1,000 machine VDI deployment during a high load session launch test.
- The Standard_A3 instance was deemed excessive for this site size, so we continue with a breakdown of the Standard_A2_v2.
- Larger VDI sites might see a requirement for using the Standard_A3.
More processes running on the Cloud Connector are not shown because they did not register meaningful metrics.

- The Citrix Remote Broker Provider (XaXdCloudProxy) handles communication between the customer-managed VDA machines and the Citrix-managed Services (Delivery Controller).
- LSASS on the Cloud Connectors processes all Active Directory authentications. The authentications made by the Citrix Cloud Services are proxied to the customer-managed Active Directory via the Cloud Connectors.
- The graph shows the usage from a single Cloud Connector that received a higher amount of load during the test. The additional Cloud Connector in the test exhibited lower CPU usage and was not included in the graph.

Cloud Connector memory usage instance comparison
• Lower available memory on the Standard_A2_v2 (4 GB memory) shows high memory utilization on the Standard_A2_v2 VM.
• The high memory utilization is caused by the Citrix Remote HCL Server (RemoteHCLServer) process that maintains the power state of the 1,000 machines in Azure.
  – Due to Azure API rate limitations, the states cannot be queried at regular intervals.
• Changes to the Citrix Remote HCL Server (RemoteHCLServer) implemented after our testing allow the Delivery Controller to communicate machine states directly to Azure.
  – The change reduces memory usage significantly and allows the Standard_A2_v2 instances to manage the 1,000 VDA site without issue.

**Session launch times**

**Comparison of the Standard_A2_v2 and Standard_A3 with customer-managed and Citrix-managed StoreFront servers**

<table>
<thead>
<tr>
<th></th>
<th>Customer-managed StoreFront*</th>
<th>Customer-managed StoreFront*</th>
<th>Citrix-managed StoreFront</th>
<th>Citrix-managed StoreFront</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3</td>
<td>561 ms</td>
<td>575 ms</td>
<td>1,996 ms</td>
<td>2,051 ms</td>
</tr>
<tr>
<td>Authenticate</td>
<td>1,132 ms</td>
<td>1,054 ms</td>
<td>1,410 ms</td>
<td>1,577 ms</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
<table>
<thead>
<tr>
<th></th>
<th>Customer-managed StoreFront*</th>
<th>Customer-managed StoreFront*</th>
<th>Citrix-managed StoreFront</th>
<th>Citrix-managed StoreFront</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total login</strong></td>
<td>1,693 ms</td>
<td>1,629 ms</td>
<td>3,406 ms</td>
<td>3,621 ms</td>
</tr>
<tr>
<td><strong>Retrieve ICA file</strong></td>
<td>3,464 ms</td>
<td>3,659 ms</td>
<td>4,730 ms</td>
<td>6,222 ms</td>
</tr>
<tr>
<td><strong>OS logon complete</strong></td>
<td>38.83 seconds</td>
<td>41.91 seconds</td>
<td>37.67 seconds</td>
<td>40.08 seconds</td>
</tr>
<tr>
<td><strong>Total launch</strong></td>
<td>42.3 seconds</td>
<td>45.6 seconds</td>
<td>42.4 seconds</td>
<td>42.4 seconds</td>
</tr>
</tbody>
</table>

Times are the average over all test runs. Customer-managed StoreFront server in Azure: Standard_DS2_v2 (2 vCPU, 7 GB Memory)

- Citrix-managed StoreFront sessions experience slower times under load because StoreFront must authenticate with the customer-managed Active Directory over the WAN.
- There were approximately 30 ms of latency between the client machines and NetScaler during testing.
- There is an average 3–4 second decrease in session launches when using a Standard_A3 instances for Cloud Connectors when the environment is under stress.
  - The Standard_A3 VM has twice as many CPU cores as the Standard_A2_v2
  - There is high memory utilization on the Standard_A2_v2 instance during the test.
    * High memory utilization was resolved when we removed the RemoteHCLServer communication from the Cloud Connectors in Azure ARM deployments.

**Session log on times for 1,000 Windows 10 sessions**
• All machines were powered on before the test.
• The test procedure started 1,000 sessions during approximately an 8-minute period.
• The average time to active desktop with a Standard_D2_v2 instance Windows 10 64-bit VDA was approximately 37.67 seconds.
• The graph shows individual logon times over the course of the test, from the time the ICA file is retrieved until an active usable desktop is presented.
  – The green and yellow areas denote one and two standard deviations, respectively.
• Although the session start times are consistent, there are some outliers. Momentary changes in network conditions can cause the outliers, impacting:
  – Secure Ticket Authority (STA) ticket exchange on the NetScaler being proxied via Cloud Connectors.
  – Establishment of an HDX connection over the WAN.
  – Azure Storage. Tests used standard storage.

**Simulated session launch**

The simulated session launch test puts stress on the Cloud Connectors, Delivery Controller, and Site database. Simulated session launch tests the capability of the components to handle a high number
of concurrent logons and to sustain those sessions under a sustained load. Session counts of 5,000 and 20,000 were tested. This document focuses on the 20,000-session tests. The launch rate and component behavior are nearly identical between the two tests. The 20,000-session test runs longer and gives a broader look at the service usage over time. 25 sessions were concurrently launched as fast as possible. The setting for launching sessions as fast as possible allowed the system under test to dictate the rate at which the environment responds to connections.

Cloud Connector HA set CPU usage during session launch test

- The graph shows a comparison of Cloud Connector CPU usage during a 20,000-session launch.
- Two Cloud Connectors are deployed for stress and load testing. An N+1 deployment of three Cloud Connectors is recommended for High Availability utilization.
- No CPU contention was observed during the test.

Cloud Connector CPU usage by component during 20,000 session launch test
• LSASS (Local Security Authority Subsystem Service) uses CPU during session logons using both Citrix-managed and customer-managed StoreFront.

• All authentications from Citrix-managed services must traverse the Cloud Connectors to communicate with the customer-managed Active Directory.

Memory usage by component during 20,000 session launch
• Memory pressure is low during session launch.
• Memory usage by most components doesn’t change throughout the test as observed by the Max and Average values being nearly equal.

Session launch comparison of the customer-managed and Citrix-managed StoreFront servers

<table>
<thead>
<tr>
<th></th>
<th>Customer-managed StoreFront*</th>
<th>Citrix-managed StoreFront</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>261 ms</td>
<td>1,629 ms</td>
</tr>
<tr>
<td>Enumerate</td>
<td>1,075 ms</td>
<td>1,275 mss</td>
</tr>
<tr>
<td>Total login</td>
<td>1,336 ms</td>
<td>2,904 ms</td>
</tr>
<tr>
<td>Retrieve ICA file</td>
<td>2,132 ms</td>
<td>2,715 ms</td>
</tr>
</tbody>
</table>

Notes:
Customer-managed StoreFront server used for testing was an 8 vCPU, 8 GB memory, 2012 R2 VM. Citrix managed StoreFront is on the Delivery Controller and shares resources with other Citrix Services.

• Usage of a customer-managed StoreFront server is faster due to the time required for AD authentication over the WAN.
• There were approximately 30 ms of latency between the Cloud Connectors and Delivery Controller during testing.
• There is a 2-second difference in the logon process using the Citrix-managed StoreFront versus a customer-managed StoreFront Server when the StoreFront server is under load.
• A 1.2-second difference in the average time to retrieve an ICA file is observed. This is an 83% increase.
• The use of a customer-managed StoreFront server is recommended for customers who require a high volume of concurrent session launches.

Machine Creation Service Provisioning

Citrix Virtual Desktops Essentials MCS testing Azure Resource Manager

The Machine Creation Service allows you to create and delete virtual desktops (VDA) in Azure. The first step is to create a Windows 10 VHD and then upload the VHD to Azure. The master image is created from the VHD. Citrix Virtual Desktops Essentials allows you to create virtual machines from the master image.
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Machine count</th>
<th>Master image copy</th>
<th>Active directory account creation</th>
<th>Machine creation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>30 mins</td>
<td>1 min</td>
<td>7 mins</td>
</tr>
<tr>
<td>100</td>
<td>30 mins</td>
<td>7 mins</td>
<td>50 mins</td>
</tr>
<tr>
<td>250</td>
<td>40 mins</td>
<td>8 mins</td>
<td>2 hours</td>
</tr>
<tr>
<td>500</td>
<td>55 mins</td>
<td>15 mins</td>
<td>4 hours</td>
</tr>
<tr>
<td>1000</td>
<td>65 mins</td>
<td>30 mins</td>
<td>8 hours</td>
</tr>
</tbody>
</table>

Times are approximate based on several test runs and may vary.

- We tested the machine creation process using various machine counts, to measure the time required to:
  - Copy the master image
  - Create machine accounts
  - Provision the machines
- The times do not increase linearly because copies of the master image must be replicated to each storage account. Replication occurs in parallel, and becomes slower with more tasks
  - There is a limit of 40 machines per storage account. The limit requires 25 storage accounts for a 1,000 VM environment.
  - There is a limit of 760 machines per resource location.
- Active Directory account creation must be proxied via the Cloud Connectors, which increases the time required to complete the task. Active Directory accounts are created at a rate of approximately 33 per minute.
- Testing used Standard_A2_v2 Cloud Connectors. No resource bottlenecks were observed.

**Citrix Virtual Apps and Desktops service MCS testing**

MCS provisioning tests were performed on a VMware ESXi 6.0 hypervisor. There are eight vSphere hosts in the cluster and share storage is NFS on a NetApp share.
Times are approximate based on multiple test runs and may vary. Test data from these runs are averaged in the table.

- The time required for the machine creation process is similar to the time required in XenApp and XenDesktop 7.x versions. The primary difference in these tests is Active Directory account creation. In the cloud environment, account creation must be proxied via the Cloud Connectors. Active Directory accounts in the cloud environment are created at a rate of approximately 33 per minute.
- We conducted the tests using two 4-vCPU, 4-GB memory VMs for the Cloud Connectors. There was no resource contention observed during the test.

**Scale and size considerations for Local Host Cache**

November 27, 2018

The Local Host Cache feature in the Citrix Virtual Apps and Desktops service allows connection brokering in a site to continue if there is an outage. An outage happens if the WAN link between the site and the management console fails in a Citrix Cloud environment. For details, see Local Host Cache. In December 2017, we tested the Citrix Cloud Connector machine configuration using the Local Host Cache feature, and a minimum of three Cloud Connectors. The test results provided in this article detail the tested maximums in December 2017. Best practice recommendations are based on those tested maximums.

Local Host Cache supports only on-premises StoreFront in each resource location or zone. The Local Host Cache feature uses only one socket for multi-core CPUs for the connector VM configuration. In this scenario, we recommend a 4-core, 1-socket configuration.

**Summary**

All results in this summary are based on the findings from test environments which we configured as detailed in the following sections. Different system configurations yield different results.

**Key recommendations based on test results:**

- We recommend, for High Availability sites that host no more than 5,000 workstations or 500 server VDAs, that you configure 3 VMs dedicated to the Cloud Connector. Each Cloud Connector VM requires 4 vCPU with 4 GB RAM. This configuration is an N+1 High Availability configuration. Cloud connectors are deployed in High Availability sets. Cloud connectors are not load-balanced. Because each CPU can process a limited number of connections, the CPU is the greatest limiting factor related to the number of workstations or server VDAs supported.
• Although this document focuses on testing with two Cloud Connectors, an N+1 set of three Cloud Connectors is recommended.
• We conducted session launch tests to compare Local Host Cache outage mode active and inactive after a new configuration was synchronized and imported. The launch tests covered scenarios with 5,000, 20,000, and 1,000 session launches against the respective number of available workstations.
  – 5,000 sessions launched against 5,000 workstation VDAs
    * Tests used 2 Cloud Connector VMs, each had 4 vCPU and 4 GB RAM. Based on the recommendation for an N+1 configuration, production environments should include 3 Cloud Connector VMs that meet these specifications.
    * Local Host Cache service peak consumed 91% of CPU resources and there was an average of 563 MB available memory.
    * It took approximately 10 minutes from when the High Availability Service detected an outage for all VDAs to re-register with the High Availability Service, which is now the broker. We measured from the time the High Availability Service entered outage mode until the High Availability Service was ready to broker sessions again.
  – 20,000 sessions launched against 500 server VDAs
    * Tests used 2 Cloud Connector VMs, each had 4 vCPU and 4 GB RAM. Based on the recommendation for an N+1 configuration, production environments should include 3 Cloud Connector VMs that meet these specifications.
    * Local Host Cache service peak consumed 90% of CPU resources and there was an average of 471 MB available memory.
    * It took approximately 8 minutes from when the High Availability Service detected an outage for all VDAs to re-register with the High Availability Service. We measured from the time the High Availability Service entered outage mode until the High Availability Service was ready to broker sessions again.
  – 1,000 sessions launched against 1,000 workstation VDAs
    * Tests used 2 Cloud Connector VMs, each had 2 vCPU and 4 GB RAM. Based on the recommendation for an N+1 configuration, production environments should include 3 Cloud Connector VMs that meet these specifications.
    * Local Host Cache service peak consumed 95% of CPU resources and there was an average of 589 MB available memory
    * It took approximately 7 minutes from when the High Availability Service detected an outage for all VDAs to re-register with the High Availability Service, which is now the broker. We measured from the time the High Availability Service entered outage mode until the High Availability Service was ready to broker sessions again.
Test methodology

We conducted tests by adding load and measuring the performance of the environment components:

- CPU
- Memory
- Database load
- Citrix Remote Broker Provider service
- Citrix High Availability Service

We collected performance data, logon time, or both. In certain cases, proprietary Citrix simulation tools were used to simulate VDAs and sessions. The simulation tools are designed to exercise Citrix components the same way that traditional VDAs and sessions do, without the same resource requirements to host real sessions and VDAs.

Local Host Cache supports one elected High Availability Service per zone, not per site. For example, if you have five zones, one connector is elected as the broker in each zone. The Citrix Config Synchronizer service is responsible for importing the Citrix-managed site database. Every configuration sync creates a database, so initial configurations are needed, such as compiling stored procedures the first time the database is used. We executed all tests after a configuration sync.

Session launch tests

On customer-managed StoreFront servers, we started 5,000 and 20,000 session tests. The monitoring tools collect StoreFront log on time, resource enumeration, and ICA file retrieval.
Citrix uses simulation tools to facilitate high-volume user testing. The simulation tools, which are proprietary to Citrix, allow us to run the tests on less hardware than is required to run tests using real sessions at these levels (5,000 and 20,000 sessions). These simulated sessions go through the normal StoreFront log on, resource enumeration, and ICA file retrieval, but do not start active desktops. Instead, the simulation tool reports to the ICA stack that the session has launched and all communication between the broker agent and the broker service is consistent with that of an actual session. Performance metrics are gathered from Citrix Cloud Connectors. To determine how the environment responded to session launches, a sustained concurrency of 25 session launches was maintained at any given time throughout the duration of the test. The measurements therefore show results of a system under load throughout the test.

**Test results**

**Session launch**

The following tables compare session launch tests between Local Host Cache outage mode active and Local Host Cache outage mode inactive after a new configuration synchronization import. Each table shows the results for the number of sessions launched in the test.

### 5,000 workstation VDA sessions

<table>
<thead>
<tr>
<th></th>
<th>Local Host Cache outage mode Inactive (normal operations) / Average timing</th>
<th>Local Host Cache outage mode Active / Average timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>193 ms</td>
<td>95 ms</td>
</tr>
<tr>
<td>Enumerate</td>
<td>697 ms</td>
<td>75 ms</td>
</tr>
<tr>
<td>Total logon time</td>
<td>890 ms</td>
<td>170 ms</td>
</tr>
<tr>
<td>Retrieve ICA File</td>
<td>4,191 ms</td>
<td>156 ms</td>
</tr>
</tbody>
</table>

### 20,000 server VDA Sessions

<table>
<thead>
<tr>
<th></th>
<th>Local Host Cache outage mode Inactive (normal operations) / Average timing</th>
<th>Local Host Cache outage mode Active / Average timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>135 ms</td>
<td>112 ms</td>
</tr>
<tr>
<td>Enumerate</td>
<td>317 ms</td>
<td>91 ms</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Local Host Cache outage mode Inactive (normal operations) / Average timing</th>
<th>Local Host Cache outage mode Active / Average timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total logon time</td>
<td>452 ms</td>
</tr>
<tr>
<td>Retrieve ICA File</td>
<td>762 ms</td>
</tr>
</tbody>
</table>

- **5,000 workstation VDA session launch test**
  - There were approximately 30 ms of latency between the Citrix Cloud Connectors and Citrix Delivery Controller while Local Host Cache outage mode was inactive.
  - There is a 720 ms difference in the logon process with Local Host Cache outage mode active versus inactive, while the StoreFront is under load.
  - The largest time difference is in the retrieval of the ICA file, which is 4 seconds. This is largely because the connector is performing the brokering, whereas normally the StoreFront traffic traverses through the connectors to the Citrix Delivery Controller in Azure and back.

- **20,000 server VDA session launch test**
  - There is a 249 ms difference in the logon process with Local Host Cache outage mode active versus inactive, while the StoreFront is under load.
  - The difference in the retrieval of the ICA file is about 1 second.

- Compared to the 5,000-workstation VDA session launch, the 20,000-session launch test contains only 500 server VDAs, resulting in fewer calls from the Citrix Delivery Controller to the VDAs, which leads to lower response times.

### Average CPU usage comparison

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average CPU %</th>
<th>Peak CPU %</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>Connector 1</td>
<td>8.3</td>
</tr>
<tr>
<td></td>
<td>Connector 2</td>
<td>8.4</td>
</tr>
<tr>
<td>5,000 workstation VDA sessions - Local Host Cache outage mode active</td>
<td>Connector 1 (elected High Availability Service)</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Connector 2</td>
<td>0.8</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>Connector 1</td>
<td>23</td>
</tr>
</tbody>
</table>
The table compares Citrix Cloud Connector CPU usage with Local Host Cache outage mode active and Local Host Cache mode inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.

- All Cloud Connectors are 4 vCPU and 4 GB RAM
- The elected High Availability Service machines peaked at 91% and 90% overall CPU respectively. It is worth noting that, while the non-elected High Availability Service does not have much usage, it may become the active if the elected High Availability Service has a failure. It is therefore critical for the connectors to have identical connector specifications.

### Available memory usage

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Connector 1</th>
<th>Connector 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>636 MB</td>
<td>786 MB</td>
</tr>
<tr>
<td>5,000 workstation VDA sessions - Local Host Cache outage mode active</td>
<td>563 MB (elected High Availability Service)</td>
<td>912 MB</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>1030 MB</td>
<td>1178 MB</td>
</tr>
</tbody>
</table>
The table compares available memory usage with Local Host Cache outage mode active and Local Host Cache mode inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.

- The number of sessions decreases the amount of available memory.
- There is a 54.35% (559 MB) increase in memory usage with 20,000 server VDA sessions when Local Host Cache outage mode is active, mainly due to SQL server memory consumption.

**Cloud Connector CPU usage by component**

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Component</th>
<th>Average CPU %</th>
<th>Peak CPU %</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>Connector 1 LSASS</td>
<td>2.4</td>
<td>10.7</td>
</tr>
<tr>
<td></td>
<td>Connector 1 XaXdCloudProxy</td>
<td>3.5</td>
<td>18.5</td>
</tr>
<tr>
<td></td>
<td>Connector 2 LSASS</td>
<td>2.5</td>
<td>12.9</td>
</tr>
<tr>
<td></td>
<td>Connector 2 XaXdCloudProxy</td>
<td>3.5</td>
<td>21.2</td>
</tr>
<tr>
<td>5,000 workstation VDA sessions Local Host Cache outage mode active</td>
<td>Connector 1 (elected High Availability Service) LSASS</td>
<td>12.9</td>
<td>29.5</td>
</tr>
<tr>
<td></td>
<td>Connector 1 (elected High Availability Service) HighAvailabilityService</td>
<td>14.7</td>
<td>49.7</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>Connector 1 LSASS</td>
<td>7</td>
<td>12.2</td>
</tr>
</tbody>
</table>
### Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Component</th>
<th>Average CPU %</th>
<th>Peak CPU %</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Connector 1 XaXdCloudProxy</td>
<td>8.7</td>
<td>15.5</td>
</tr>
<tr>
<td></td>
<td>Connector 2 LSASS</td>
<td>7</td>
<td>12.5</td>
</tr>
<tr>
<td></td>
<td>Connector 2 XaXdCloudProxy</td>
<td>9</td>
<td>15.7</td>
</tr>
<tr>
<td>20,000 sessions Local Host Cache outage mode active</td>
<td>Connector 1 (elected High Availability Service) LSASS</td>
<td>4.3</td>
<td>17.2</td>
</tr>
<tr>
<td></td>
<td>Connector 1 (elected High Availability Service) High Availability Service</td>
<td>4.5</td>
<td>18.2</td>
</tr>
</tbody>
</table>

- The preceding table shows the processes that consume the most overall CPU resources when Local Host Cache outage mode is active, compared to when Local Host Cache outage mode is inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.

- The Citrix Remote Broker Provider service (XaXdCloudProxy) is the top CPU consumer when Local Host Cache outage mode is inactive.

- LSASS (Local Security Authority Subsystem Service) uses CPU during session logons. All authentications from Citrix-managed services must traverse the Citrix Cloud Connectors to communicate with the customer-managed Active Directory.

- The Citrix High Availability Service is used to broker the sessions, resulting in higher CPU usage when Local Host Cache outage mode is active. Also, CPU usage peaked to 49.7% during the 5,000 workstation VDA session launch, while the usage was only 18.25% during the 20,000 server VDA session launch (500 VDAs). The difference is due to the number of VDAs.

- Connector 2 did not have any meaningful metrics, as it was not the elected High Availability Service.

#### VDA re-registration time while switching to Local Host Cache

During a Delivery Controller outage, the 5,000 workstation VDAs must re-register with the elected Local Host Cache broker. This re-registration time was ~10 minutes. The re-registration time for 500 server VDAs was ~8 minutes.
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Number of VDAs</th>
<th>Re-registration time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDAs</td>
<td>~10 minutes</td>
</tr>
<tr>
<td>500 server VDAs</td>
<td>~8 minutes</td>
</tr>
</tbody>
</table>

### Outage timings

<table>
<thead>
<tr>
<th>Outage event</th>
<th>Number of VDAs</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter outage mode</td>
<td></td>
<td>10 minutes</td>
</tr>
<tr>
<td>Re-registration time to elected High Availability Service</td>
<td>500</td>
<td>~8 minutes</td>
</tr>
<tr>
<td></td>
<td>5000</td>
<td>~10 minutes</td>
</tr>
<tr>
<td>Exit outage mode</td>
<td></td>
<td>10 minutes</td>
</tr>
<tr>
<td>Re-registration time to Citrix Delivery Controller</td>
<td>500</td>
<td>~5.5 minutes</td>
</tr>
<tr>
<td></td>
<td>5000</td>
<td>~1.5 minutes</td>
</tr>
</tbody>
</table>

- There is a total of 20 minutes to enter (10 minutes) and exit (10 minutes) outage mode, due to the number of Citrix Delivery Controller health checks required. The time required to re-register the VDAs adds to the overall outage time.
- If the network is going up and down repeatedly, forcing an outage until the network issues resolve prevents continuous transition between normal and outage modes.

### Database and High Availability Service metrics with Local Host Cache

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average High Availability Service Database Transactions/sec</th>
<th>Peak High Availability Service Database Transactions/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>436</td>
<td>1344</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>590</td>
<td>2061</td>
</tr>
</tbody>
</table>

The preceding table shows the number of database transactions per second on the elected High Availa-
ability Service.

**StoreFront CPU usage comparison**

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average CPU %</th>
<th>Peak CPU %</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>4.5</td>
<td>32.4</td>
</tr>
<tr>
<td>5,000 server VDA sessions</td>
<td>13.8</td>
<td>32.6</td>
</tr>
<tr>
<td>Local Host Cache outage mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>11.4</td>
<td>22.1</td>
</tr>
<tr>
<td>20,000 server VDA sessions - Local Host Cache outage mode</td>
<td>18.6</td>
<td>33.2</td>
</tr>
</tbody>
</table>

- The preceding table compares StoreFront CPU usage when Local Host Cache outage mode is active to when Local Host Cache mode is inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.
- The StoreFront machine has the following specifications: Windows 2012 R2, 8 vCPU (2 sockets, 4 cores each), 8 GB RAM
- When Local Host Cache outage mode is active, there is approximately a 9% increase in average CPU usage with the 5,000 workstation VDA and about a 7% increase with the 20,000 server VDA session launch tests. The increase is mostly because the IIS worker processes more requests when Local Host Cache outage mode is active. There is more CPU usage because StoreFront is processing session launches at a faster rate than when outage mode is inactive.

**StoreFront available memory usage comparison**

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average available memory (working set MB)</th>
<th>Peak available memory (working set MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>5731</td>
<td>6821</td>
</tr>
<tr>
<td>5,000 workstation VDA sessions Local Host Cache outage mode</td>
<td>5345</td>
<td>5420</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>4671</td>
<td>4924</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average available memory (working set MB)</th>
<th>Peak available memory (working set MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20,000 server VDA sessions - Local Host Cache outage mode</td>
<td>4730</td>
<td>5027</td>
</tr>
</tbody>
</table>

- The preceding table compares the StoreFront available memory usage when Local Host Cache outage mode is active and when Local Host Cache mode is inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.
- When Local Host Cache mode is active, there is a 6.73% increase in memory usage during the 5,000 workstation VDA session launch test.

The following table compares outage mode active vs inactive after a new configuration synchronization import, launching 1,000 sessions to 1,000 workstation VDAs with Local Host Cache, and using Citrix Cloud Connectors configured with 2 vCPU VMs.

**Session launch comparison**

<table>
<thead>
<tr>
<th></th>
<th>Local Host Cache outage mode inactive (normal operations)</th>
<th>Local Host Cache outage mode active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>359 ms</td>
<td>89 ms</td>
</tr>
<tr>
<td>Enumerate</td>
<td>436 ms</td>
<td>180 ms</td>
</tr>
<tr>
<td>Total logon time</td>
<td>795 ms</td>
<td>269 ms</td>
</tr>
<tr>
<td>Retrieve ICA File</td>
<td>804 ms</td>
<td>549 ms</td>
</tr>
</tbody>
</table>

- While the StoreFront is under load, there is a 526 ms difference in the logon process when Local Host Cache outage mode is active compared to when Local Host Cache mode is inactive.
- There is a 255 ms difference in the retrieval of the ICA file when Local Host Cache outage mode is active compared to when Local Host Cache mode is inactive. The difference increases with the number of sessions.

**Average CPU usage comparison**
The elected High Availability Service peaked to 95% overall CPU, which indicates that 1,000 workstation VDA is an optimal configuration for a 2 vCPU connector VM.

**Average memory usage comparison**

The preceding graph displays a comparison of Citrix Cloud Connector available usage when Local Host
Cache outage mode is active versus inactive, during a 1,000 workstation VDA session launch. There is not a significant difference in memory based on the Local Host Cache outage mode.

**Cloud Connector CPU usage by component comparison**

The preceding graph displays the processes that consume the most CPU resources while Local Host Cache outage mode is inactive.
• The preceding graph displays the processes that consume the most CPU resources when Local Host Cache outage mode is active.
• Connector 2 did not have any meaningful metrics.

**VDA re-registration time while switching to Local Host Cache**

During a Delivery Controller outage, the 1000 workstation VDAs must re-register with the elected Local Host Cache broker. The re-registration time was ~7 minutes.

**Database and High Availability Service metrics with Local Host Cache**
The preceding graph displays the number of database transactions per second on the elected High Availability Service.

**Impact with increasing number of zones on database import times**

An extra zone (with a pair of its own connectors) was added to the test site to understand the impact. The first zone consists of 5,500 unique objects (2 catalogs). The secondary zone is a mirror of the first zone, and has its own unique objects, totaling 11,000 objects. It is important to note that Local Host Cache is recommended only for zones with no more than 10,000 objects. Before we added the secondary zone, database import time on the connectors was about 4 minutes, 20 seconds. After we added the secondary zone and populated it with 11,000 objects, the import time increased to by ~30 seconds to ~4 minutes, 50 seconds. Adding more catalogs has marginal impact on import times. The largest contributing factors to performance degradation and increased import times are based on the number of assigned machines, users, and remote PCs. Additionally, 5,500 objects were split between 2 zones and the import time remained the same.

<table>
<thead>
<tr>
<th>Number of zones</th>
<th>Total Number of Objects</th>
<th>Import time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5,500</td>
<td>4 minutes 20 seconds</td>
</tr>
<tr>
<td>2</td>
<td>11,000</td>
<td>4 minutes 50 seconds</td>
</tr>
<tr>
<td>2</td>
<td>5,500</td>
<td>4 minutes 20 seconds</td>
</tr>
</tbody>
</table>
**Connector sizing guidance**

For optimal performance, the following are the recommended configurations for Citrix Cloud Connector when Local Host Cache mode is enabled.

**Recommendation 1:** to support 1,000 workstation VDAs using Local Host Cache mode with Citrix Cloud Connector

- 2 Windows 2012 R2 VMs, each allocated with 2 vCPU (1 socket, 2 cores), 4 GB RAM
- This recommended sizing is based on the peak Citrix Cloud Connector overall 95% CPU usage and 589 MB average available memory while Local Host Cache mode is active

**Recommendation 2:** to support 5,000 workstation VDAs OR 500 server VDAs using Local Host Cache with Citrix Cloud Connector

- 2 Windows 2012 R2 VMs, each allocated with 4 vCPU (1 socket, 4 cores), 4 GB RAM
- This recommended sizing is based on
  - 5,000 workstation VDA sessions launched with Local Host Cache mode active
    * Overall 91% peak CPU usage
    * 563 MB average available memory
  - 20,000 server VDA sessions launched with Local Host Cache mode active
    * Overall 90% peak CPU usage
    * 471 MB average available memory

See [Scale and size considerations for Cloud Connectors](#) for more information about general scalability sizing.

**Test environment**

The test environment employed internally developed, proprietary testing tools, and VMs configured to the specifications in the following sections.

**Tools used**

We used an internal testing tool to collect performance data and metrics from the machines under test and to drive the session launches. The in-house testing tool orchestrates user session launches to the Citrix Virtual Apps and Desktops environment. The testing tool also provides a central location where we gather response time data and performance metrics. In essence, the test tool administers the tests and collects the results.

**Test configuration – Citrix Virtual Apps and Desktops service**

The following is a list of the machine and OS specifications used with the Citrix Virtual Apps and Desktops service testing.
Citrix Virtual Apps and Desktops service

- **Cloud Connectors:**
  - 2 Windows 2012 R2 VMs, each allocated 4 vCPU (1 socket, 4 cores), 4 GB RAM
  - 2 Windows 2012 R2 VMs, each allocated 2 vCPU (1 socket, 2 cores), 4 GB RAM
- **StoreFront (customer-managed):** Windows 2012 R2, 8 vCPU (2 sockets, 4 cores each), 8 GB RAM
- **Hypervisor:** Citrix XenServer 7.0 + updates, 5x HP Blade BL 460C Gen 9, 2x Intel E5-2620 CPU, 256 GB RAM
- **Hypervisor Storage:** 2 TB NFS share on NetApp 3250
- **VDA:** Windows 2012 R2

**Data collection**

We collect the following metrics from each test:

- Average overall CPU, memory, component (cloud processes) usage increase
- VDA re-registration time when switching to the elected Local Host Cache High Availability Service
- Database and High Availability Service metrics when Local Host Cache outage mode is active
- Session launch comparison, average timings for:
  - Authentication
  - Enumeration
  - ICA file retrieval
- Impact to database synchronization times while increasing the number of zones
  - Time required to synchronize after a configuration change

**Create and manage connections**

May 22, 2019

**Introduction**

Configuring a connection includes selecting the connection type from among the supported hypervisors and cloud services. The storage and network you select form the resources for that connection. You must be a Full Administrator to perform connection and resource management tasks.

**Where to find information about connection types**

*System requirements* lists the supported hypervisor and cloud service versions, and includes links to
Host storage

A storage product is supported if it can be managed by a supported hypervisor. Citrix Support will assist those storage product vendors in troubleshooting and resolving issues, and document those issues in the knowledge center, as needed.

When provisioning machines, data is classified by type:

- Operating system (OS) data, which includes master images.
- Temporary data, which includes all non-persistent data written to MCS-provisioned machines, Windows page files, user profile data, and any data that is synchronized with Content Collaboration (formerly ShareFile). This data is discarded each time a machine restarts.
- Personal data stored on personal vDisks.

Providing separate storage for each data type can reduce load and improve IOPS performance on each storage device, making best use of the host’s available resources. It also enables appropriate storage to be used for the different data types; persistence and resilience is more important for some data than others.

- Storage can be shared (located centrally, separate from any host, used by all hosts) or local to a hypervisor. For example, central shared storage could be one or more Windows Server 2012 clustered storage volumes (with or without attached storage), or an appliance from a storage vendor. The central storage might also provide its own optimizations such as hypervisor storage control paths and direct access through partner plugins.
- Storing temporary data locally avoids having to traverse the network to access shared storage. This also reduces load (IOPS) on the shared storage device. Shared storage can be more costly, so storing data locally can lower expenses. These benefits must be weighed against the availability of sufficient storage on the hypervisor servers.

Storage shared by hypervisors

The storage shared by hypervisors method stores data that needs longer-term persistence centrally, providing centralized backup and management. That storage holds the OS disks and the personal vDisk disks.

When you select this method, you can choose whether to use local storage (on servers in the same hypervisor pool) for temporary machine data that does not require persistence or as much resilience as the data in the shared storage. This is called the temporary data cache. The local disk helps reduce traffic to the main OS storage. This disk is cleared after every machine restart. The disk is accessed
through a write-through memory cache. Keep in mind that if you use local storage for temporary data, the provisioned VDA is tied to a specific hypervisor host; if that host fails, the VM cannot start.

**Exception:** If you use Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager does not allow temporary data cache disks to be created on local storage.

When you create a connection, if you enable the option to store temporary data locally, you can then enable and configure nondefault values for each VM’s cache disk size and memory size when you create a machine catalog that uses that connection. However, the default values are tailored to the connection type, and are sufficient for most cases.

The hypervisor can also provide optimization technologies through read caching of the disk images locally; for example, Citrix Hypervisor offers IntelliCache. This can also reduce network traffic to the central storage.

**Storage local to the hypervisor**

The storage local to the hypervisor method stores data locally on the hypervisor. With this method, master images and other OS data are transferred to all of the hypervisors used in the Site, both for initial machine creation and future image updates. This results in significant traffic on the management network. Image transfers are also time-consuming, and the images become available to each host at a different time.

When you select this method, you can choose whether to use shared storage for personal vDisks, to provide resilience and support for backup and disaster recovery systems.

**Create a connection and resources**

**Important:**

The host resources (storage and network) in your resource location must be available before you create a connection.

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > Virtual Apps and Desktops**.
3. Click **Manage**. Studio opens. If a connection has not been created yet, you are guided to that step.
4. Select **Configuration > Hosting** in the navigation pane.
5. Select **Add Connections and Resources** in the Actions pane.
6. The wizard guides you through the following pages. Specific page content depends on the selected connection type. After completing each page, click **Next** until you reach the **Summary** page.
**Step 1. Connection**

On the **Connection** page:

- To create a new connection select **Create a new Connection**. To create a connection based on the same host configuration as an existing connection, select **Use an existing Connection** and then choose the relevant connection.
- Select the hypervisor or cloud service you are using in the **Connection type** field.
- The connection address and credentials fields differ, depending on the selected connection type. Enter the requested information.
- Enter a connection name. This name will appear in Studio.
- Choose the tool you will use to create virtual machines: Studio tools or other tools.

Information on the **Connection** page differs depending on the host (connection type) you’re using. For example, when using Azure Resource Manager, you can use an existing service principal or create a new one. For details, see the virtualization environment page listed above for your connection type.
Step 2. Storage management

For information about storage management types and methods, see Host storage.

If you are configuring a connection to a Hyper-V or VMware host, browse to and then select a cluster name. Other connection types do not request a cluster name.

Select a storage management method: storage shared by hypervisors or storage local to the hypervisor.

- If you choose storage shared by hypervisors, indicate if you want to keep temporary data on available local storage. (You can specify nondefault temporary storage sizes in the Machine Catalogs that use this connection.) **Exception:** When using Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager does not allow temporary data cache disks to be created on local storage, so configuring that storage management setup in Studio will fail.
- If you choose storage local to the hypervisor, indicate if you want to manage personal data on shared storage.

If you use shared storage on a Citrix Hypervisor pool, indicate if you want to use IntelliCache to reduce the load on the shared storage device. See Citrix Hypervisor virtualization environments.
Step 3. Storage selection

For more information about storage selection, see Host storage.

Select at least one host storage device for each available data type. The storage management method you selected on the previous page affects which data types are available for selection on this page. You must select at least one storage device for each supported data type before you can proceed to the next page in the wizard.

The lower portion of the Storage Selection page contains additional configuration options if you selected either of the following on the previous page:

- If you chose storage shared by hypervisors, and enabled the Optimize temporary data on available local storage check box, you can select which local storage devices (in the same hypervisor pool) to use for temporary data.
- If you chose storage local to the hypervisor, and enabled the Manage personal data centrally on shared storage check box, you can select which shared devices to use for personal (PvD) data.

The number of currently selected storage devices is shown (in the graphic above, “1 storage device selected”). When you hover over that entry, the selected device names appear (unless there are no devices configured).
1. Click **Select** to change the storage devices to use.
2. In the **Select Storage** dialog box, select or clear the storage device check boxes, and then click **OK**.

**Step 4. Region**

The connection wizard for some connection types (such as Azure Resource Manager) contain a **Region** page. The region selection controls where VMs will be deployed. Ideally, choose a region close to where users will access their applications.

**Step 5. Network**

Enter a name for the resources; this name appears in Studio to identify the storage and network combination associated with the connection.

Select one or more networks that the VMs will use.

Some connection types (such as Azure Resource Manager) also list subnets that VMs will use. Select one or more subnets.

**Step 6. Summary**

Review your selections; if you want to make changes, use return to previous wizard pages. When you complete your review, click **Finish**.

**Remember**: If you chose to store temporary data locally, you can configure nondefault values for temporary data storage when you create the machine catalog containing machines that use this connection.

**Edit connection settings**

Do not use this procedure to rename a connection or to create a new connection. Those are different operations. Change the address only if the current host machine has a new address; entering an address to a different machine will break the connection's machine catalogs.

You cannot change the GPU settings for a connection, because catalogs accessing this resource must use an appropriate GPU-specific master image. Create a new connection.

1. From Studio, select **Configuration > Hosting** in the navigation pane.
2. Select the connection and then select **Edit Connection** in the Actions pane.
3. Follow the guidance below for the settings available when you edit a connection.
4. When you are finished, click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

**Connection Properties** page:

- To change the connection address and credentials, select **Edit settings** and then enter the new information.
- To specify the high-availability servers for a Citrix Hypervisor connection, select **Edit HA servers**. Citrix recommends that you select all servers in the pool to allow communication with Citrix Hypervisor if the pool master fails.

**Advanced** page:

The throttling threshold settings enable you to specify a maximum number of power actions allowed on a connection. These settings can help when power management settings allow too many or too few machines to start at the same time. Each connection type has specific default values that are appropriate for most cases and should generally not be changed.

- The **Simultaneous actions (all types)** and **Simultaneous Personal vDisk inventory updates** settings specify two values: a maximum absolute number that can occur simultaneously on this connection, and a maximum percentage of all machines that use this connection. You must specify both absolute and percentage values; the actual limit applied is the lower of the 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).

- The **Maximum new actions per minute** is an absolute number; there is no percentage value.

Enter information in the **Connection options** field 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. From Studio, select **Configuration > Hosting** in the 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. Additionally, you can turn maintenance mode on or off for machines in machine catalogs or Delivery Groups.
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 deleting 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 used by the connection are powered off.

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.

1. From Studio, select Configuration > Hosting in the 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.

Rename or test a connection

1. From Studio, select Configuration > Hosting in the navigation pane.
2. Select the connection and then select Rename Connection or Test Connection in the Actions pane.

View machine details on a connection

1. From Studio, select Configuration > Hosting in the 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. From Studio, select Configuration > Hosting in the navigation pane.
2. Select a connection and then select View Machines in the Actions 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:** Temporarily stops connections to a machine. Users cannot connect to a machine in this state. If users are connected, maintenance mode takes effect when they log off. (You can also turn maintenance mode on or off for all machines accessed through a connection, as described 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.

Edit storage

You can display the status of servers that are used to store operating system, temporary, and personal (PvD) data for VMs that use a connection. You can also specify which servers to use for storage of each data type.

1. From Studio, select Configuration > Hosting in the navigation pane.
2. Select the connection and then select Edit Storage in the Actions pane.
3. In the left pane, select the data type: operating system, personal vDisk, or temporary.
4. Select or clear the checkboxes for one or more storage devices for the selected data type.
5. Click **OK**.

Each storage device in the list includes its name and storage status. Valid storage status values are:

- **In use**: The storage is being used for creating new machines.
- **Superseded**: The storage is being used only for existing machines. No new machines will be added in this storage.
- **Not in use**: The storage is not being used for creating machines.

If you clear the check box for a device that is currently **In use**, its status changes to **Superseded**. Existing machines will continue to use that storage device (and can write data to it), so it is possible for that location to become full even after it stops being used for creating new machines.

### Delete, rename, or test resources

1. From Studio, select **Configuration > Hosting** in the navigation pane.
2. Select the resource and then select the appropriate entry in the Actions pane: **Delete Resources**, **Rename Resources**, or **Test Resources**.

### Connection timers

You can use Citrix policy settings to configure three connection timers:

- **Maximum connection timer**: 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.
- **Connection idle timer**: 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.
- **Disconnect timer**: 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.

See the policy settings documentation for more information.

### Where to go next

If you’re in the initial deployment process, create a machine catalog.
This article begins with a description of VDAs and the available VDA installers. The remainder of the article describes the steps in the VDA installation wizard. Command-line equivalents are provided. For details, see Install VDAs using the command line.

About VDAs

The Citrix Virtual Apps and Desktops service article describes what VDAs are and what they do. Here’s more information.

- **Analytics collection**: Analytics are collected automatically when you install (or upgrade) components. By default, that data is uploaded to Citrix automatically when the installation completes. Also, when you install components, you are automatically enrolled in the Citrix Customer Experience Improvement Program (CEIP), which uploads anonymous data. For information about these programs, see Citrix Insight Services.
- **Citrix Workspace app**: Citrix Workspace app for Windows is not installed by default when you install a VDA. You or your users can download and install (and upgrade) Citrix Workspace app for Windows and other Citrix Workspace apps from the Citrix website. Alternatively, you can make those Citrix Workspace apps available from the Workspace or a StoreFront server.
- **Print Spooler Service**: The Print Spooler Service is enabled by default on supported Windows Servers. If you disable this service, you cannot successfully install a VDA for Server OS, so ensure that this service is enabled before installing a VDA.
- **Microsoft Media Foundation**: Most supported Windows editions come with Media Foundation already installed. If the machine on which you’re installing a VDA does not have Microsoft Media Foundation (such as N editions), several multimedia features will not be installed and will not work. You can acknowledge the limitation, or end the VDA installation and restart it later, after installing Media Foundation. In the graphical interface, this choice is presented in a message. In the command line, you can use the /no_mediafoundation_ack option to acknowledge the limitation. If Media Foundation is not present on the VDA, these multimedia features do not work:
  - Flash Redirection
  - Windows Media Redirection
  - HTML5 Video Redirection
  - HDX RealTime Webcam Redirection
- **Local user group**: When you install the VDA, a new local user group called Direct Access Users is created automatically. On a VDA for Desktop OS, this group applies only to RDP connections. On a VDA for Server OS, this group applies to ICA and RDP connections.
• **Cloud Connector address requirement:** The VDA must have at least one valid Cloud Connector address (in the same resource location) with which to communicate. Otherwise, sessions cannot be established. You specify Cloud Connector addresses when you install the VDA. For information about other ways to specify Cloud Connector addresses where VDAs can register, see VDA registration.

• **Operating system considerations:**
  - Review the System requirements for supported platforms, operating systems, and versions.
  - Ensure that each operating system maintains the latest updates.
  - Ensure that VDAs have synchronized system clocks. The Kerberos infrastructure that secures communication between the machines requires synchronization.
  - Optimization guidance for Windows 10 machines is available in CTX216252.
  - If you try to install (or upgrade to) a Windows VDA on an OS that is not supported for that VDA version, a message describes your options. For example, if you try to install the latest VDA on a Windows 7 machine, a message guides you to CTX139030. For more information, see Earlier operating systems.

**VDA supportability tools**

Each VDA installer includes a supportability MSI that contains Citrix tools for checking the VDA’s performance, such as its overall health and the quality of connections. Enable or disable installation of this MSI on the Additional Components page of the VDA installer’s graphical interface. From the command line, you can disable installation with the /exclude "Citrix Supportability Tools" option.

By default, the supportability MSI is installed in C:\Program Files (x86)\Citrix\Supportability Tools. You can change this location on the Components page of the VDA installer’s graphical interface, or with the /installdir command-line option. Keep in mind that changing the location changes it for all installed VDA components, not just the supportability tools.

Current tools in the supportability MSI:

- Citrix Health Assistant: For details, see CTX207624.
- VDA Cleanup Utility: For details, see CTX209255.

If you do not install the tools when you install the VDA, the CTX article contains a link to the current download package.

**Restarts during VDA installation**

A restart is required at the end of the VDA installation. That restart occurs automatically by default. To minimize the number of restarts needed during VDA installation:
• Ensure that a supported .NET Framework version is installed before beginning the VDA installation.
• For Windows Server OS machines, install and enable the RDS role services before installing the VDA.

If you do not install those prerequisites before installing the VDA:

• If you are using the graphical interface or the command line interface without the /noreboot option, the machine restarts automatically after installing the prerequisite.
• If you are using the command line interface with the /noreboot option, you must initiate the restart.

After each restart, the VDA installation continues. If you’re installing from the command line, you can prevent the automatic resumption with the /noresume option.

When upgrading a VDA to version 7.17 or a later supported version, a restart occurs during the upgrade. This cannot be avoided.

VDA installers

VDA installers can be downloaded directly from the Citrix Cloud console.

By default, files in the self-extracting installers are extracted to the Temp folder. The files extracted to the Temp folder are automatically deleted after the installation completes. Alternatively, you can use the/extract command with an absolute path.

Three standalone VDA installers are available for download.

VDAServerSetup.exe

Installs a VDA for Server OS.

VDAWorkstationSetup.exe

Installs a VDA for Desktop OS.

VDAWorkstationCoreSetup.exe

Installs a VDA for Desktop OS that is optimized for Remote PC Access deployments or core VDI installations. Remote PC Access uses physical machines. Core VDI installations are VMs that are not being used as a master image. This installer deploys only the core services necessary for VDA connections. Therefore, it supports only a subset of the options that are valid with the VDAWorkstationSetup installer.
This installer does not install or contain the components used for:

- App-V.
- Profile Management. Excluding Citrix Profile Management from the installation affects Monitor displays.
- Machine Identity Service.
- Personal vDisk or AppDisks.
- Citrix Workspace app for Windows.
- Citrix Supportability Tools.
- Citrix Files for Windows.
- Citrix Files for Outlook.

This installer does not install or contain a Citrix Workspace app for Windows.

Using VDAWorkstationCoreSetup.exe is equivalent to using the VDAWorkstationSetup installer to install a Desktop OS VDA and either:

- In the graphical interface: Selecting the **Remote PC Access** option on the **Environment** page.
- In the command line interface: Specifying the `/remotepc` option.
- In the command line interface: Specifying `/components vda` and `/exclude "Citrix Personalization for App-V - VDA""Personal vDisk""Machine Identity Service""Citrix User Profile Manager""Citrix User Profile Manager WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows""Citrix Files for Outlook"`.

If you originally install a VDA with the VDAWorkstationCoreSetup.exe installer and later upgrade that VDA using the VDAWorkstationSetup.exe installer, you can optionally install the omitted components and features.

### Install a VDA

Ensure that the machine is domain-joined before installing the VDA software.

#### Step 1. Download the product software and launch the wizard

1. On the machine where you’re installing the VDA, sign in to **Citrix Cloud**.
2. In the upper left menu, select **My Services > Virtual Apps and Desktops**.
3. On the right side, click **Downloads** and select **Download VDA**. You are redirected to the VDA download page. Find the VDA installer you want and then click **Download File**.
4. After the download completes, right-click the file and select **Run as administrator**. The installation wizard launches.

As an alternative to steps 1-3, you can download the VDA directly from the **Citrix download page**.
**Step 2. Specify how the VDA will be used**

On the **Environment** page, specify how you plan to use the VDA, indicating whether you’ll use this machine as a master image to provision machines. The option you choose affects which Citrix provisioning tools are installed automatically (if any), and the default values on the **Additional Components** page of the VDA installer. Several MSIs (provisioning and other) are installed automatically when you install a VDA. The only way to prevent their installation is with the `/exclude` option in a command-line installation.

Choose one of the following:

- **Create a master MCS image**: Select this option to install a VDA on a VM master image, if you plan to use Machine Creation Services to provision VMs. This option installs the Machine Identity Service, which includes TargetOSOptimizer.exe. This is the default option. Command-line option: `/mastermcsimage` or `/masterimage`
- **Create a master image using Citrix Provisioning or third-party provisioning tools**: Select this option to install a VDA on a VM master image, if you plan to use Citrix Provisioning or third-party provisioning tools (such as Microsoft System Center Configuration Manager). Command-line option: `/masterpvsimage`
- **(Appears only on server OS machines) Enable brokered connections to a server**: Select this
Citrix Virtual Apps and Desktops service

option to install a VDA on a physical or virtual machine that will not be used as a master image. Command-line option: /remotecpc

- (Appears only on desktop OS machines) **Enable Remote PC Access**: Select this option to install a VDA on a physical machine for use with Remote PC Access. Command-line option: /remotecpc

Click **Next**.

This page does not appear:

- If you’re upgrading a VDA
- If you are using the VDAWorkstationCoreSetup.exe installer

**Step 3. Select the components to install and the installation location**

On the **Core components** page:

- **Location**: By default, components are installed in C:\Program Files\Citrix. This default is fine for most deployments. If you specify a different location, that location must have execute permissions for network service. Command-line option: /installdir

- **Components**: By default, Citrix Workspace app for Windows is not installed with the VDA. If you are using the VDAWorkstationCoreSetup.exe installer, Citrix Workspace app for Windows is
never installed, so this check box is not displayed. Command-line option: /components vda, plugin to install the VDA and the Citrix Workspace app for Windows

Click Next.

**Step 4. Install additional components**

The Additional Components page contains check boxes to enable or disable installation of other features and technologies with the VDA. In a command-line installation, you can use the /exclude or /include additional option to expressly omit or include one or more available components.

The following table indicates the default setting of items on this page. The default setting depends on the option you selected on the Environment page.
### Additional Components page

<table>
<thead>
<tr>
<th>Environment page: “Master image with MCS” or “Master image with Citrix Provisioning…” selected</th>
<th>Environment page: “Enable brokered connections to server” (for server OS) or “Remote PC Access” (for desktop OS) selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Personalization for App-V</td>
<td>Not selected</td>
</tr>
<tr>
<td>Citrix AppDisk/Personal vDisk</td>
<td>Not selected</td>
</tr>
<tr>
<td>Citrix Supportability tools</td>
<td>Selected</td>
</tr>
<tr>
<td>Citrix User Profile Manager</td>
<td>Selected</td>
</tr>
<tr>
<td>Citrix User Profile Manager WMI Plugin</td>
<td>Selected</td>
</tr>
<tr>
<td>Citrix Files for Windows</td>
<td>Not selected</td>
</tr>
<tr>
<td>Citrix Files for Outlook</td>
<td>Not selected</td>
</tr>
</tbody>
</table>

This page does not appear if:

- You are using the VDAWorkstationCoreSetup.exe installer. Also, the command-line options for the additional components are not valid with that installer.
- You are upgrading a VDA and all the additional components are already installed. (If some of the additional components are already installed, the page lists only the components that are not installed.)

The components list can include:

- **Citrix Personalization for App-V**: Install this component if you use applications from Microsoft App-V packages. For details, see App-V.
  
  Command-line option: `/includeadditional "Citrix Personalization for App-V - VDA"` to enable component installation, `/exclude "Citrix Personalization for App -V - VDA"` to prevent component installation

- **Citrix AppDisk / Personal vDisk**: These technologies are deprecated. Valid only when installing a VDA for Desktop OS on a VM. Installs components used for AppDisk and Personal vDisk.
  
  Command-line option: `/includeadditional "Personal vDisk"` to enable component installation, `/exclude "Personal vDisk"` to prevent AppDisk and Personal vDisk component installation

- **Citrix Supportability Tools**: Installs the MSI that contains Citrix supportability tools, such as the Citrix Health Assistant.
Command-line option: `/includeadditional "Citrix Supportability Tools"` to enable component installation, `/exclude "Citrix Supportability Tools"` to prevent component installation

- **Citrix User Profile Manager**: This component manages user personalization settings in user profiles. For details, see Profile Management.

Excluding Citrix Profile Management from the installation affects the monitoring and troubleshooting of VDAs in Citrix Cloud. On the **User details** and **EndPoint** pages of the Monitor tab, the Personalization panel and the Logon Duration panel fail. On the Dashboard and Trends pages, the Average Logon Duration panel display data only for machines that have Profile Management installed.

Even if you are using a third-party user profile management solution, Citrix recommends that you install and run the Citrix Profile Management Service. Enabling the Citrix Profile Management Service is not required.

Command-line option: `/includeadditional "Citrix User Profile Manager"` to enable component installation, `/exclude "Citrix User Profile Manager"` to prevent component installation

- **Citrix User Profile Manager WMI Plugin**: This plug-in provides Profile Management runtime information in WMI (Windows Management Instrumentation) objects (for example, profile provider, profile type, size, and disk usage). WMI objects provide session information to Director.

Command-line option: `/includeadditional "Citrix User Profile Manager WMI Plugin"` to enable component installation, `/exclude "Citrix User Profile Manager WMI Plugin"` to prevent component installation

- **Citrix Files for Windows**: This component enables users to connect to their Citrix Files account. They can then interact with Citrix Files through a mapped drive in the Windows file system (without requiring a full sync of their content).

Command-line options: `/includeadditional "Citrix Files for Windows"` to enable component installation, `/exclude "Citrix Files for Windows"` to prevent component installation

- **Citrix Files for Outlook**: This component allows you to bypass file size restrictions and add security to your attachments or emails by sending them through Citrix Files. You can provide a secure file upload request for co-workers, customers, and partners directly in your email. For more information, see Citrix Files for Outlook.

Command-line options: `/includeadditional "Citrix Files for Outlook"` to enable component installation, `/exclude "Citrix Files for Outlook"` to prevent component installation
Step 5. Cloud Connector addresses

On the Delivery Controller page, select Do it manually. Enter the DNS name of an installed Cloud Connector and then click Add. If you’ve installed additional Cloud Connectors in the resource location, add their DNS names.

Click Next.

Considerations:

- The address can contain only alphanumeric characters.
- Successful VDA registration requires that the firewall ports used to communicate with the Cloud Connector are open. That action is enabled by default on the Firewall page of the wizard.

Command-line option: /controllers
Step 6. Enable or disable features

On the Features page, use the check boxes to enable or disable features you want to use.

- **Optimize performance:** When you use MCS and enable this feature (default), VM optimization disables offline files, disables background defragmentation, and reduces event log size. For details, see CTX125874.

  In addition to enabling this feature, optimization requires that the Machine Identity Service be installed. That service contains the TargetOSOptimizer.exe file. The Machine Identity Service is installed automatically when you:
  
  - In the graphical interface, select Create a master MCS image on the Environment page.
  - In the command-line interface, specify /mastermcsimage or /masterimage (and do not specify /exclude "Machine Identity Service").

  Command-line option: /optimize

If you are using the VDAWorkstationCoreSetup.exe installer, this feature does not appear in the wizard, and the command-line option is not valid.

In a Remote PC Access environment, disable this feature.

- **Use Windows Remote Assistance:** When this feature is enabled, Windows Remote Assistance is used with the user shadowing feature of the Director component in Citrix Cloud. Windows Remote Assistance opens the dynamic ports in the firewall. (Default = disabled)

  Command-line option: /enable_remote_assistance
• **Use Real-Time Audio Transport for audio:** Enable this feature if voice-over-IP is widely used in your network. The feature reduces latency and improves audio resilience over lossy networks. It allows audio data to be transmitted using RTP over UDP transport. (Default = disabled)

Command-line option: `/enable_real_time_transport`

• **AppDisk / Personal vDisk:** These technologies are deprecated. Valid only when installing a VDA for Desktop OS on a VM. This check box is available only if the Citrix AppDisk / Personal vDisk check box is selected on the Additional Components page. When this check box is enabled, AppDisks and Personal vDisks can be used.

Command-line option: `/baseimage`

If you are using the VDAWorkstationCoreSetup.exe installer, this feature does not appear in the wizard and the command-line option is not valid.

• **MCS I/O:** Valid only when using MCS to provision VMs. When selected, the MCSIO write caching driver is installed. For more information, see Storage shared by hypervisors and Configure cache for temporary data.

Command-line option: `/install_mcsio_driver`

**Important:**

This feature is not enabled by default (so the driver is not installed). You must install that driver to use the MCS temporary data caching feature.

Click *Next*. 
Step 7. Firewall ports

The **Firewall** page indicates which ports the VDA and Cloud Connectors use to communicate with each other. By default, these ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. This default setting is fine for most deployments. For port information, see [Network ports](#).

Click **Next**.

Command-line option: `/enable_hdx_ports`
**Step 8. Review prerequisites and confirm installation**

The **Summary** page lists what will be installed. You can return to earlier wizard pages and change selections.

When you’re ready, click **Install**.

If prerequisites aren’t already installed/enabled, the machine might restart once or twice. See [Prepare to install](#).
Step 9. Diagnose

On the Diagnostics page, choose whether to participate in Citrix Call Home. If you choose to participate (the default), click Connect. When prompted, enter your Citrix account credentials.

After your credentials are validated (or if you choose not to participate), click Next.

For more information, see Call Home.
Step 10. Complete this installation

The Finish page contains green check marks for all prerequisites and components that installed and initialized successfully.

Click Finish. By default, the machine restarts automatically. (Although you can disable this automatic restart, the VDA cannot be used until the machine restarts.)

If you are installing a VDA on individual machines (rather than a master image), repeat the steps above to install a VDA on other machines, as needed.

Troubleshoot

In the Studio display for a Delivery Group, the Installed VDA version entry in the details pane might not be the version installed on the machines. The machine’s Windows Programs and Features display shows the actual VDA version.

Customize a VDA

Later, to customize (change information for) an installed VDA:
1. From the Windows feature for removing or changing programs, select Citrix Virtual Delivery Agent or Citrix Remote PC Access/VDI Core Services VDA. Then right-click and select Change.

2. Select Customize Virtual Delivery Agent Settings. When the installer launches, you can change:
   - Cloud Connector addresses
   - TCP/IP port to register with the Controller (default = 80)
   - Whether to open Windows Firewall ports automatically

Where to go next

Create machine catalogs

To review the entire configuration process, see Install and configure.

Install VDAs using the command line

July 9, 2019

This article applies to installing, upgrading, and customizing Virtual Delivery Agents (VDAs) on machines with Windows operating systems.

This article describes how to issue VDA installation commands. Before beginning an installation, review Install VDAs to learn about installation considerations, installers, and what you specify during installation.

Install a VDA

Ensure that the machine is domain-joined before installing the VDA software.

To install a VDA (and see command execution progress and return values), you must have elevated administrative privileges or use Run as administrator.

1. On the machine where you’re installing the VDA, sign to Citrix Cloud.
2. In the upper left menu, select My Services > Virtual Apps and Desktops.
3. On the upper right side, click Downloads and select Download VDA. You are redirected to the VDA download page. Find the VDA installer you want and click Download File.
4. After the download completes, run its name. Use the options described in this article.
   - For the Server OS Virtual Delivery Agent, run VDAServerSetup.exe
Citrix Virtual Apps and Desktops service

- For the Desktop OS Virtual Delivery Agent, run `VDAWorkstationSetup.exe`
- For the Desktop OS Core Services Virtual Delivery Agent, run `VDAWorkstationCoreSetup.exe`

To extract the files before installing them, use `/extract` with the absolute path, for example: `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. (The directory must exist. Otherwise, the extract fails.) Then in a separate command, run `VDAWorkstationCoreSetup.exe` from the directory containing the extracted content (in the previous example, CitrixVDAInstallMedia). Use the valid options listed in this article.

**Command-line options to install a VDA**

The following options are valid with one or more of the commands: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, and `VDAWorkstationCoreSetup.exe`.

- `/baseimage`
  This technology is deprecated. Valid only when installing a VDA for Desktop OS on a VM. Enables the use of Personal vDisks with a master image.
  
  This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer.

- `/components component[,component]`
  Comma-separated list of components to install or remove. Valid values are:
  - `VDA`: Virtual Delivery Agent
  - `PLUGINS`: Citrix Workspace app for Windows
  
  To install the VDA and Citrix Workspace app, specify `/components vda,plugins`.
  
  This option is not valid when using the `VDAWorkstationCoreSetup.exe` installer. That installer cannot install Citrix Workspace app.

- `/controllers “controller [controller]…”`
  Space-separated FQDNs of Citrix Cloud Connectors with which the VDA can communicate, enclosed in straight quotation marks. Do not specify both the `/site_guid` and `/controllers` options.

- `/disableexperiencemetrics`
  Prevents the automatic upload of analytics collected during installation, upgrade, or removal to Citrix.

- `/enable_hdx_ports`
Opens ports in the Windows firewall required by the Cloud Connector and enabled features (except Windows Remote Assistance), 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. For port information, see Network ports.

To open the UDP ports that HDX adaptive transport uses to communicate with the Controller, specify the /enable_hdx_udp_ports option, in addition to the /enable_hdx_ports option.

- **/enable_hdx_udp_ports**

  Opens UDP ports in the Windows firewall that are required by HDX adaptive transport, 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. For port information, see Network ports.

  To open the ports that the VDA uses to communicate with the Controller and enabled features, specify the /enable_hdx_ports option, in addition to the /enable_hdx_udp_ports option.

- **/enable_real_time_transport**

  Enables or disables use of UDP for audio packets (RealTime 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 when the Windows Firewall Service is detected.

- **/enable_remote_assistance**

  Enables the shadowing feature in Windows Remote Assistance for use with the Monitor functions. If you specify this option, Windows Remote Assistance opens the dynamic ports in the firewall.

- **/exclude “component”[,”component”]**

  Prevents installation of one or more comma-separated optional components, each enclosed in straight quotation marks. For example, installing or upgrading a VDA on an image that is not managed by MCS does not require the Machine Identity Service component. Valid values are:

  - AppDisks VDA Plug-in
  - Personal vDisk
  - Machine Identity Service
  - Citrix User Profile Manager
  - Citrix User Profile Manager WMI Plugin
  - Citrix Universal Print Client
  - Citrix Telemetry Service
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix Files for Windows
  - Citrix Files for Outlook
Excluding Citrix Profile Management from the installation (/exclude "Citrix User Profile Manager") affects monitoring and troubleshooting of VDAs from the Monitor tab. On the User details and EndPoint pages, the Personalization panel and the Logon Duration panel fail. On the Dashboard and Trends pages, the Average Logon Duration panel display data only for machines that have Profile Management installed.

Even if you are using a third-party user profile management solution, Citrix recommends that you install and run the Citrix Profile Management Service. Enabling the Citrix Profile Management Service is not required.

If you plan to use MCS to provision VMs, do not exclude the Machine Identity Service.

If you specify both /exclude and /includeadditional with the same component name, the component is not installed.

This option is not valid when using the VDAWorkstationCoreSetup.exe installer. That installer automatically excludes many of these items.

- /h or /help
  Displays command help.

- /hdxflashv2only
  Prevents installation of Flash redirection legacy binaries, for enhanced security.
  This option is not available in the graphical interface.

- /includeadditional "component"[,"component"] …
  Includes installation of one or more comma-separated optional components, each enclosed in straight quotation marks. This option can be helpful when you are creating a Remote PC Access deployment, and want to install components that are not included by default. Valid values are:
    - Personal vDisk
    - Citrix User Profile Manager
    - Citrix User Profile Manager WMI Plugin
    - Citrix Universal Print Client
    - Citrix Telemetry Service
    - Citrix Personalization for App-V - VDA
    - Citrix Supportability Tools
    - Citrix Files for Windows
    - Citrix Files for Outlook
  If you specify both /exclude and /includeadditional with the same component name, that component is not installed.

- /installdir directory
  Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.
- **/install_mcsio_driver**
  Enables MCS I/O write cache for storage optimization.

- **/logpath path**
  Log file location. The specified folder must exist. The installer does not create it. Default = “%TEMP%\Citrix\XenDesktop Installer”
  This option is not available in the graphical interface.

- **/masterimage**
  Valid only when installing a VDA on a VM. Sets up the VDA as a master image. This option is equivalent to /mastermcsimage.
  This option is not valid when using the VDAWorkstationCoreSetup.exe installer.

- **/mastermcsimage**
  Specifies that this machine will be used as a master image with Machine Creation Services. This option also installs TargetOSOptimizer.exe (unless you also specify exclude ”Machine Identity Service” which includes the optimizer installer). This option is equivalent to /masterimage.

- **/masterpvimage**
  Specifies that this machine will be used as a master image with either Citrix Provisioning or a third-party provisioning tool (such as Microsoft System Center Configuration Manager).

- **/no_mediafoundation_ack**
  Acknowledges that Microsoft Media Foundation is not installed, and several HDX multimedia features will not be installed and will not work. If this option is omitted and Media Foundation is not installed, the VDA installation fails. Most supported Windows editions come with Media Foundation already installed, except N editions.

- **/nodesktopexperience**
  Valid only when installing a VDA for Server OS. Prevents enabling of the Enhanced Desktop Experience feature. This feature is also controlled with the Enhanced Desktop Experience Citrix policy setting.

- **/noreboot**
  Prevents a restart after installation. The VDA cannot be used until after a restart.

- **/noresume**
  By default, when a machine restart is needed during an installation, the installer resumes automatically after the restart completes. To override the default, specify /noresume. This can be
helpful if you must re-mount the media or want to capture information during an automated installation.

• **/optimize**

When you use MCS and enable this feature (default), VM optimization disables offline files, disables background defragmentation, and reduces event log size. For details, see CTX125874.

In addition to enabling this feature, optimization requires that the Machine Identity Service be installed. That service contains the TargetOSOptimizer.exe. The Machine Identity Service is installed automatically when you specify /mastermcsimage or /masterimage (and do not specify /exclude "Machine Identity Service").

• **/portnumber** \textit{port}

Valid only when the \textit{/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.

• **/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.

• **/reconfigure**

Customizes previously configured VDA settings when used with the \textit{/portnumber}, \textit{/controllers}, or \textit{/enable_hdx_ports} options. If you specify this option without also specifying the \textit{/quiet} option, the graphical interface for customizing the VDA launches.

• **/remotepc**

Valid only for Remote PC Access deployments (desktop OS) or brokered connections (server OS). Excludes installation of the following components:

- Citrix Personalization for App-V
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin
- Machine Identity Service
- Personal vDisk
- Citrix Supportability Tools
- Citrix Files for Windows
- Citrix Files for Outlook

This option is not valid when using the \textit{VDAWorkstationCoreSetup.exe} installer. That installer automatically excludes installation of these components.
Citrix Virtual Apps and Desktops service

- **/remove**
  Removes the components specified with the /components option.

- **/removeall**
  Removes all installed VDA components.

- **/sendexperiencemetrics**
  Automatically sends analytics collected during the installation, upgrade, or removal to Citrix. If this option is omitted (or the /disableexperiencemetrics option is specified), analytics are collected locally, but not sent automatically.

- **/servervdi**
  Installs a VDA for Desktop OS on a supported Windows server. Omit this option when installing a VDA for Server OS on a Windows server. Before using this option, see Server VDI.

  This option is not available in the graphical interface.

- **/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.

- **/tempdir directory**
  Directory to hold temporary files during installation. Default = c:\Windows\Temp.

  This option is not available in the graphical interface.

- **/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.

  This option is not available in the graphical interface.

**Examples: Install a VDA**

The following command installs a VDA on a server OS. The VDA will be used as a master image.

```cmd
VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/enable_hdx_ports /masterimage
```

The following command installs a Core Services VDA on a Desktop OS for use in a Remote PC Access or VDI deployment. Citrix Workspace app and other non-core services are not installed. The address of a
Cloud Connector is specified, and ports in the Windows Firewall Service will be opened automatically. The administrator will handle restarts.

VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.domain.com"/enable_hdx_ports /noreboot

Customize a VDA using the command line

After you install a VDA, you can customize several settings. Run XenDesktopVDASetup.exe, using one or more of the following options.

- /reconfigure (required when customizing a VDA)
- /h or /help
- /quiet
- /noreboot
- /controllers
- /portnumber port
- /enable_hdx_ports

Where to go next

Create machine catalogs

To review the entire configuration process, see Install and configure.

Create machine catalogs

September 20, 2019

Collections of physical or virtual machines are managed as a single entity called a machine catalog. All the machines in a catalog have the same type of operating system: multi-session OS or single session OS. A catalog containing multi-session OS machines can contain either Windows or Linux machines, not both.

Note:

If you are using Azure Resource Manager to host your resources, you can optionally use the Azure Quick Deploy deployment method, instead of using Studio as described in this article. For details, see Azure Quick Deploy.
Citrix Virtual Apps and Desktops service

Studio guides you to create the first machine catalog. After you create the first catalog, Studio guides you to create the first Delivery Group. Later, you can change the catalog you created, and create more catalogs.

Overview

When you create a catalog of VMs, you specify how to provision those VMs. You can use Citrix tools such as Machine Creation Services (MCS) or Citrix Provisioning. Or, you can use your own tools to provide machines.

- If you use Citrix Provisioning to create machines, see the Citrix Provisioning documentation for instructions.
- If you use MCS to provision VMs, you provide a master image (or snapshot) to create identical VMs in the catalog. Before you create the catalog, you first use hypervisor or cloud service tools to create and configure the master image. This process includes installing a Virtual Delivery Agent (VDA) on the image. Then you create the machine catalog in the Studio management console. You select that image (or a snapshot of an image), specify the number of VMs to create in the catalog, and configure additional information.
- If your machines are already available (so you do not need master images), you must still create one or more machine catalogs for those machines.

When using MCS to create the first catalog, you specify a host connection that you created previously. Later (after you create your first catalog and Delivery Group), you can change information about that connection or create more connections.

If a Cloud Connector is not operating properly, MCS provisioning operations (such as catalog updates) take much longer than usual, and Studio performance degrades significantly.

RDS license check

Creation of a machine catalog containing Windows multi-session OS machines includes an automatic check for valid Microsoft RDS licenses. Studio searches the catalog for a powered-on and registered machine to perform the check on.

- If a powered-on and registered machine cannot be found, a warning is displayed, explaining that the RDS licensing check could not be performed.
- If a machine is found and an error is detected, Studio displays a warning message for the catalog containing the detected issue. To remove an RDS license warning from a catalog (so that it no longer appears in the Studio display), select the catalog. Click Remove RDS license warning in the Actions pane. When prompted, confirm the action.
VDA registration

A VDA must be registered with a Cloud Connector to be considered when launching brokered sessions. Unregistered VDAs can result in underutilization of otherwise available resources. There are various reasons a VDA might not be registered, many of which you can troubleshoot. Studio provides troubleshooting information in the catalog creation wizard, and after you add a catalog to a Delivery Group.

In the catalog creation wizard, after you add existing machines, the list of computer account names indicates whether each machine is suitable for adding to the catalog. Hover over the icon next to each machine to display an informative message about that machine.

If the message identifies a problematic machine, you can either remove that machine (using the Remove button), or add the machine. For example, if a message indicates that information could not be obtained about a machine (perhaps because it had never registered), you might choose to add the machine anyway.

For more information about VDA registration troubleshooting, see CTX136668.

MCS catalog creation summary

Here’s a brief overview of default MCS actions after you provide information in the catalog creation wizard.

- If you selected a master image (rather than a snapshot), MCS creates a snapshot.
- MCS creates a full copy of the snapshot and places the copy on each storage location defined in the host connection.
- MCS adds the machines to Active Directory, which creates unique identities.
- MCS creates the number of VMs specified in the wizard, with two disks defined for each VM. In addition to the two disks per VM, a master is also stored in the same storage location. If you have multiple storage locations defined, each gets the following disk types:
  - The full copy of the snapshot (noted above), which is read-only and shared across the just-created VMs.
  - A unique 16 MB identity disk that gives each VM a unique identity. Each VM gets an identity disk.
  - A unique difference disk to store writes made to the VM. This disk is thin provisioned (if supported by the host storage) and increases to the maximum size of the master image, if necessary. Each VM gets a difference disk. The difference disk holds changes made during sessions. It is permanent for dedicated desktops. For pooled desktops, it is deleted and a new one created after each restart.

Alternatively, when creating VMs to deliver static desktops, you can specify (on the Machines page of the catalog creation wizard) thick (full copy) VM clones. Full clones do not require retention of the
master image on every data store. Each VM has its own file.

**Prepare a master image on the hypervisor or cloud service**

The master image contains the operating system, non-virtualized applications, VDA, and other software.

Good to know:

- A master image might also be known as a clone image, golden image, base VM, or base image. Host vendors and cloud service providers may use different terms.
- When using Citrix Provisioning, you can use a master image or a physical computer as the master target device. Citrix Provisioning uses different terminology than MCS to refer to images; see the [Citrix Provisioning](/en-us/provisioning.html) documentation for details.
- Ensure that the hypervisor or cloud service has enough processors, memory, and storage to accommodate the number of machines created.
- Configure the correct amount of hard disk space needed for desktops and applications. That value cannot be changed later or in the machine catalog.
- Remote PC Access machine catalogs do not use master images.
- Microsoft KMS activation considerations when using MCS: 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 rearm Microsoft Windows or Microsoft Office.

Install and configure the following software on the master image:

- Integration tools for your hypervisor (such as Citrix VM Tools, Hyper-V Integration Services, or VMware tools). If you omit this step, applications and desktops might not function correctly.
- A VDA. Citrix recommends installing the latest version to allow access to the newest features. Failure to install a VDA on the master image causes the catalog creation to fail.
- Third-party tools as needed, such as anti-virus software or electronic software distribution agents. Configure services with settings that are appropriate for users and the machine type (such as updating features).
- Third-party applications that you are not virtualizing. Citrix recommends virtualizing applications. Virtualizing reduces costs by eliminating having to update the master image after adding or reconfiguring an application. Also, 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. The App-V client is available from Microsoft.
- When using MCS, if you 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.
Important:
If you are using Citrix Provisioning or MCS, do not run Sysprep on master images.

To prepare a master image:

1. Using your hypervisor’s management tool, create a master image and then install the operating system, plus all service packs and updates. Specify the number of vCPUs. You can also specify the vCPU value if you create the machine catalog using PowerShell. You cannot specify the number of vCPUs when creating a catalog using Studio. Configure the amount of hard disk space needed for desktops and applications. That value cannot be changed later or in the catalog.

2. Ensure that the hard disk is attached at device location 0. Most standard master image templates configure this location by default, but some custom templates might not.

3. Install and configure the software listed above on the master image.

4. When using Citrix Provisioning, create a VHD file for the vDisk from your master target device before you join the master target device to a domain. See the Citrix Provisioning documentation for details.

5. If you are not using MCS, join the master image to the domain where applications and desktops are members. Ensure that the master image is available on the host where the machines are created. If you are using MCS, joining the master image to a domain is not required. The provisioned machines are joined to the domain specified in the catalog creation wizard.

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 catalog, Studio creates a snapshot, but you cannot name it.

Start creating the catalog

Before creating a catalog:

- Review this section to learn about the choices you make and information you supply.
- Ensure that you have created a connection to the hypervisor, cloud service, other resource that hosts your machines.
- If you have created a master image to provision machines, ensure that you have installed a VDA on that image.

To start the catalog creation wizard:

1. Sign in to Citrix Cloud. In the upper left menu, select My Services > Virtual Apps and Desktops.
2. Click Manage.
3. If this is the first catalog being created, Studio guides you to the correct selection (such as “Set up the machines and create machine catalogs to run apps and desktops.”). The catalog creation wizard opens and walks you through the items described below.
If you already created a catalog and want to create another, select **Machine Catalogs** in the **Studio** navigation pane. Then select **Create Machine Catalog** in the **Actions** pane.

The wizard walks you through the pages described below. The pages you see may differ, depending on the selections you make, and the connection (to a host) you use. **Hosts / virtualization resouces** lists information sources for the supported host types.

### Operating system

Each catalog contains machines of only one type:

- **Multi-session OS**: A multi-session OS catalog provides hosted shared desktops. The machines can be running supported versions of the Windows or Linux operating systems, but the catalog cannot contain both.
- **Single session OS**: A single session OS catalog provides VDI desktops that you can assign to various different 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.

### Machine management

This page does not appear when you are creating a Remote PC Access catalog.

The **Machine Management** page indicates how machines are managed and which tool you use to deploy machines.

Choose if 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 already configured a connection to a hypervisor or cloud service.
- Machines are not power managed through Studio, for example, physical machines.

If you indicated that machines are power managed through Studio or provisioned through a cloud environment, choose which tool to use to create VMs.

- **Citrix Machine Creation Services (MCS)**: Uses a master image to create and manage virtual machines. Machine catalogs in cloud environments use MCS. MCS is not available for physical machines.
- **Citrix Provisioning**: Manages target devices as a device collection. A Citrix Provisioning vDisk imaged from a master target device delivers desktops and applications. This option is not available for cloud deployments.
Citrix Virtual Apps and Desktops service

- **Other**: A tool that manages machines already in the data center. Citrix recommends that you use Microsoft System Center Configuration Manager or another third-party application to ensure that the machines in the catalog are consistent.

**Desktop types (desktop experience)**

This page appears only when you are creating a catalog containing single session OS machines.

The **Desktop Experience** page determines what occurs each time a user logs on. Select one of:

- Users connect to a new (random) desktop each time they log on.
- Users connect to the same (static) desktop each time they log on.

If you choose the second option and are using Citrix Provisioning to provision the machines, you can configure how user changes to the desktop are handled:

- Save user changes to the desktop on a separate Personal vDisk.
- Save user changes to the desktop on the local disk.
- Discard user changes and clear the virtual desktop when the user logs off.

**Master image**

This page appears only when you are using MCS to create VMs.

Select the connection to the host hypervisor or cloud service, and then select the snapshot or VM created earlier.

Remember:

- When you are using MCS or Citrix Provisioning, do not run Sysprep on master images.
- If you specify a master image rather than a snapshot, Studio creates a snapshot, but you cannot name it.

Do not change the default minimum VDA version selection.

An error message appears if you select a snapshot or VM that is not compatible with the machine management technology you selected earlier in the wizard.

**Cloud platform and service environments**

When you are using a cloud service or platform to host VMs, the catalog creation wizard may contain extra pages specific to that host. For example, when using an Azure Resource Manager master image, the catalog creation wizard contains a **Storage and License Types** page.

For host-specific information, follow the appropriate link listed in Start creating the catalog.
Device Collection

This page appears only when using Citrix Provisioning to create VMs. It displays the device collections and the devices that have not already been added to catalogs.

Select the device collections to use. See the Citrix Provisioning documentation for details.

Machines

This page does not appear when you are creating Remote PC Access catalogs.

The title of this page depends on what you selected on the Machine Management page: Machines, Virtual Machines, or VMs and users.

- **When using MCS to create machines:**
  - Specify how many virtual machines to create.
  - Choose the amount of memory (in MB) each VM has.
  - **Important:** Each created VM has a hard disk. Its size is set in the master image; you cannot change the hard disk size in the catalog.
  - If you indicated on the Desktop Experience page that user changes to static desktops should be saved on a separate Personal vDisk, specify the vDisk size in gigabytes and the drive letter.
  - If your deployment uses more than one zone (resource location), you can select a zone for the catalog.
  - If you are creating static desktop VMs, select a virtual machine copy mode. See Virtual machine copy mode.
  - If you are creating random desktop VMs that do not use personal vDisks, you can configure a cache to be used for temporary data on each machine. See Configure cache for temporary data.

- **When using Citrix Provisioning to create machines:**

  The Devices page lists the machines in the device collection that you selected on the previous wizard page. You cannot add or remove machines on this page.

- **When using other tools to provide machines:**

  Add (or import a list of) Active Directory machine account names. You can change the Active Directory account name for a VM after you add/import it. If you specified static machines on the Desktop Experience wizard page, you can optionally specify the Active Directory user name for each VM you add.

  After you add or import names, you can use the Remove button to delete names from the list, while you are still on this wizard page.
When using Citrix Provisioning or other tools (but not MCS):

An icon and tooltip for each machine added (or imported, or from a Citrix Provisioning device collection) help identify machines that might not be eligible to add to the catalog, or be unable to register with a Cloud Connector.

Virtual machine copy mode

The copy mode you specify on the Machines page determines whether MCS creates thin (fast copy) or thick (full copy) clones from the master image. (Default = thin clones)

- Use fast copy clones for more efficient storage use and faster machine creation.
- Use full copy clones for better data recovery and migration support, with potentially reduced IOPS after the machines are created.

Configure cache for temporary data

Caching temporary data locally on the VM is optional. You can enable use of the temporary data cache on the machine when you use MCS to manage pooled (not dedicated) machines in a catalog. If the catalog uses a connection that specifies storage for temporary data, you can enable and configure the temporary data cache information when you create the catalog.

To enable the caching of temporary data, the VDA on each machine in the catalog must be minimum version 7.9. This feature is referred to as MCSIO.

Important:
This feature requires a current MCSIO driver. Installing this driver is an option when you install or upgrade a VDA. By default, that driver is not installed.

You specify whether temporary data uses shared or local storage when you create the connection that the catalog uses. For details, see Connections and resources. Enabling and configuring the temporary cache in the catalog includes two check boxes and values: Memory allocated to cache (MB) and Disk cache size (GB). By default, these check boxes are cleared. When you enable one or both check boxes, the default values differ according to the connection type. Generally, the default values are sufficient for most cases; however, take into account the space needed for:

- Temporary data files created by Windows itself, including the Windows page file.
- User profile data.
- ShareFile data that is synced to users’ sessions.
- Data that may be created or copied by a session user or any applications users may install inside the session.

Windows will not allow a session to use an amount of cache disk that is larger than the amount of free space on the original master image from which machines in the machine catalog are provisioned. For
example, there is no benefit specifying a 20 GB cache disk if there is only 10 GB of free space on the master image.

If you enable the **Disk cache size** check box, temporary data is initially written to the memory cache. When the memory cache reaches its configured limit (the **Memory allocated to cache** value), the oldest data is moved to the temporary data cache disk.

![Diagram showing disk and memory cache](image)

The memory cache is part of the total amount of memory on each machine; therefore, if you enable the **Memory allocated to cache** check box, consider increasing the total amount of memory on each machine.

If you clear the **Memory allocated to cache** check box and leave the **Disk cache size** check box enabled, temporary data is written directly to the cache disk, using a minimal amount of memory cache.

Changing the **Disk cache size** from its default value can affect performance. The size must match user requirements and the load placed on the machine.

**Important:**
If the disk cache runs out of space, the user’s session becomes unusable.

If you clear the **Disk cache size** check box, no cache disk is created. In this case, specify a **Memory allocated to cache** value that is large enough to hold all of the temporary data. This is feasible only if large amounts of RAM are available for allocation to each VM.

If you clear both check boxes, temporary data is not cached. It is written to the difference disk (located in the OS storage) for each VM. (This is the provisioning action in releases earlier than 7.9.)

Do not enable caching if you intend to use this catalog to create AppDisks.

You cannot change the cache values in a machine catalog after it is created.
Network Interface Cards (NICs)

This page does not appear when you are creating Remote PC Access catalogs.

If you plan to use multiple 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 page.

Machine accounts

This page appears only when creating Remote PC Access catalogs.

Specify the Active Directory machine accounts or Organizational Units (OUs) to add that correspond to users or user groups. Do not use a forward slash (/) in an OU name.

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

This page appears only when using MCS to create VMs.

Each machine in the catalog must have a corresponding Active Directory computer account. Indicate whether to create accounts or use existing accounts, and the location for those accounts.

- If you create accounts, you must have access to a domain administrator account for the domain where the machines reside.

  Specify the account naming scheme for the machines that will be created, using hash marks to indicate where sequential numbers or letters appear. Do not use a forward slash (/) in an OU name. 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, and so on.

- If you use existing accounts, either browse to the accounts or click Import and specify a .csv file containing account names. The imported file content must use the format:

  [ADComputerAccount]
  ADcomputeraccountname.domain

Ensure 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.
Citrix Virtual Apps and Desktops service

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 Citrix Provisioning, computer accounts for target devices are managed differently; see the Citrix Provisioning documentation.

Summary, name, and description

On the Summary page, review the settings you specified. Enter a name and description for the catalog. This information appears in Studio. When you’re done, click Finish to start the catalog creation.

More information

- Citrix Virtual Apps and Desktops Image Management
- Connections and resources
- Manage machine catalogs

Where to go next

If this is the first catalog created, Studio guides you to create a Delivery Group. To review the entire configuration process, see Install and configure.

Manage machine catalogs

September 20, 2019

Introduction

You can add or remove machines from a machine catalog, as well as rename, change the description, or manage a catalog’s Active Directory computer accounts. Maintaining catalogs can also include making sure each machine has the latest OS updates, anti-virus software updates, operating system upgrades, or configuration changes.

- Catalogs containing pooled random machines created using Machine Creation Services (MCS) maintain machines by updating the master image used in the catalog and then updating the machines. This method enables you to efficiently update large numbers of user machines.
Citrix Virtual Apps and Desktops service

- For machines created using Citrix Provisioning, updates to machines are propagated through the vDisk. See the Citrix Provisioning documentation for details.
- For catalogs containing static, permanently assigned machines, and for Remote PC Access Machine catalogs, you manage updates to users’ machines outside of Studio. Perform this task either individually or collectively using third-party software distribution tools.

For information about creating and managing connections to host hypervisors and cloud services, see Connections and resources.

**Note:**

MCS does not support Windows 10 IoT Core and Windows 10 IoT Enterprise. Refer to the Microsoft site for more information.

### About persistent instances

When updating an MCS catalog created using persistent, or dedicated instances, any new machines created for the catalog use the updated image. Pre-existing instances continue to use the original instance. The process of updating an image is done the same way for any other type of catalog. Consider the following:

- With persistent disk catalogs, the pre-existing machines are not updated to the new image, but any new machines added to the catalog use the new image.
- For non-persistent disk catalogs, the machine image is updated the next time the machine is reset.
- With persistent machine catalogs, updating the image also updates the catalog instances that use it.
- For catalogs that do not persist, if you want different images for different machines, the images must reside in separate catalogs.

### Add machines to a catalog

**Before you start:**

- Make sure the virtualization host (hypervisor or cloud service provider) has sufficient processors, memory, and storage to accommodate the additional machines.
- Make sure that you have enough unused Active Directory computer accounts. If you are using existing accounts, the number of machines you can add is limited by the number of accounts available.
- If you use Studio to create Active Directory computer accounts for the additional machines, you must have appropriate domain administrator permission.

**To add machines to a catalog:**
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 there are insufficient existing Active Directory accounts for the number of VMs you are adding, select the domain and location where the accounts are created. Specify an account naming scheme, using hash marks to indicate where sequential numbers or letters appear. Do not use a forward slash (/) in an OU name. 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, and so on.
5. If you use existing Active Directory accounts, 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. 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 take much time when creating many machines. Machine creation continues even if you close Studio.

**Delete machines from a catalog**

After you delete a machine from a machine catalog, users can no longer access it, so before deleting a machine, ensure that:

- User data is backed up or no longer required.
- All users are logged off. Turning on maintenance mode stops new connections from being made to a machine.
- Machines are powered off.

To delete machines from a catalog:

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 select **Delete** in the **Actions** pane.

Choose whether to delete the machines being removed. If you choose to delete the machines, indicate whether the Active Directory accounts for those machines should be retained, disabled, or deleted.

When you delete an Azure Resource Manager machine catalog, the associated machines and resource groups are deleted from Azure, even if you indicate that they should be retained.

**Change a catalog description or change Remote PC Access settings**

1. Select **Machine Catalogs** in the **Studio** navigation pane.
Citrix Virtual Apps and Desktops service

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 the power management settings and select a power management connection. On the **Organizational Units** page, add or remove Active Directory OUs.
4. On the **Description** page, change the catalog description.

**Rename a catalog**

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.

**Move a catalog to a different zone**

If your deployment has more than one zone, you can move a catalog from one zone to another.

Keep in mind that moving a catalog to a different zone than the hypervisor or cloud service containing the VMs in that catalog can affect performance.

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a catalog and then select **Move** in the **Actions** pane.
3. Select the zone where you want to move the catalog.

**Delete a catalog**

Before deleting a 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 so that new connections cannot be made.
- All machines in the catalog are powered off.
- The catalog is not associated a Delivery Group. In other words, the Delivery Group does not contain machines from the catalog.

To delete a catalog:

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 Active Directory computer accounts for those machines should be retained, disabled, or deleted.
Manage Active Directory computer accounts in a catalog

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 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. Do not use a forward slash (/) in an OU name.

To manage Active Directory accounts:

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select a catalog and then select **Manage AD accounts** in the **Actions** pane.
3. Choose whether to add or delete computer accounts. If you add accounts, 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 is changed on the accounts as they are imported. If you delete an account, choose whether the account in Active Directory should be kept, disabled, or deleted.

You can also indicate whether Active Directory accounts should be retained, disabled, or deleted when you remove machines from a catalog or delete a catalog.

Update a catalog

Citrix recommends that you save copies or snapshots of master images before you update the machines in the catalog. The database keeps a historical record of the master images used with each machine catalog. Roll back, or revert, machines in a catalog to use the previous version of the master image. Perform this task if users encounter problems with updates you deployed to their desktops, minimizing user downtime. Do not delete, move, or rename master images; otherwise, you cannot revert a catalog to use them.

For catalogs that use Citrix Provisioning (formerly Provisioning Services), you must publish a new vDisk to apply changes to the catalog. For details, see the Citrix Provisioning documentation.

After a machine is updated, it restarts automatically.

Update or create a master image

Before you update the Machine Catalog, either update an existing master image or create a one on your host hypervisor.
1. On your hypervisor or cloud service provider, take a snapshot of the current VM and give the snapshot a meaningful name. This snapshot can be used to revert (roll back) machines in the catalog, if needed.

2. If necessary, power on the master image, and log on.

3. Install updates or make any required changes to the master image.

4. If the master image uses a personal vDisk, update the inventory.

5. Power off the VM.

6. Take a snapshot of the VM, and give the snapshot a meaningful name that is recognized when the catalog is updated in Studio. 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.

**Update the catalog**

To prepare and roll out the update to all machines in a catalog:

1. Select **Machine Catalogs** in the **Studio** navigation pane.

2. Select a catalog and then select **Update Machines** in the **Actions** pane.

3. On the **Master Image** page, select the host and the image you want to roll out.

4. On the **Rollout Strategy** page, choose when the machines in the Machine Catalog are updated with the new master image: on the next shutdown or immediately.

5. Verify the information on the **Summary** page and then click **Finish**. Each machine restarts automatically after it is updated.

If you are updating a catalog using the PowerShell SDK directly, rather than Studio, you can specify a hypervisor template (VMTemplates), as an alternative to an image or a snapshot of an image.

**Rollout strategy:**

Updating the image on the next shutdown is provided when you are using the Citrix Connector for System Center Configuration Manager.

If you choose to update the image immediately, configure a distribution time and notifications.

- **Distribution time:** You can choose to update all machines at the same time, or specify the total length of time it should take to begin updating all machines in the catalog. An internal algorithm determines when each machine is updated and restarted during that interval.

- **Notification:** In the left notification dropdown, choose whether to display a notification message on the machines before an update begins. By default, no message is displayed. If you choose to display a message 15 minutes before the update begins, you can choose (in the right dropdown) to repeat the message every five minutes after the initial message. By default, the
message is not repeated. Unless you choose to update all machines at the same time, the notification message displays on each machine at the appropriate time before the update begins, calculated by an internal algorithm.

**Roll back an update**

After you roll out an updated/new master image, you can roll it back. This might be necessary if issues occur with the newly updated machines. When you roll back, machines in the catalog are rolled back to the last working image. Any new features that require the newer image will no longer be available. As with the rollout, rolling back a machine includes a restart.

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select the catalog and then select **Rollback machine update** in the **Actions** pane.
3. Specify when to apply the earlier master image to machines, as described above for the rollout operation.

The rollback is applied only to machines that need to be reverted. For machines that have not been updated with the new/updated master image (for example, machines with users who have not logged off), users do not receive notification messages and are not forced to log off.

**Upgrade a catalog or revert an upgrade**

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 to enable access to all the newest features.

Before upgrading a catalog:

- If you’re using Citrix Provisioning, upgrade the VDA version in the Citrix Provisioning console.
- Start the upgraded machines so that they register with the Controller. This lets Studio determine that the machines in the catalog need upgrading.

To upgrade a catalog:

1. Select **Machine Catalogs** in the **Studio** navigation pane.
2. Select the 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 catalog to ensure that all machines function properly.

After the catalog upgrade completes, you can revert the machines to their previous VDA versions by selecting the catalog and then selecting **Undo** in the **Actions** pane.
Troubleshoot

- For machines with “Power State Unknown” status, see CTX131267 for guidance.
- If a Cloud Connector is not operating properly, MCS provisioning operations (such as catalog updates) take much longer than usual and Studio performance degrades significantly.

Azure Quick Deploy

September 9, 2019

In the Citrix Virtual Apps and Desktops service, if your resource location uses Azure Resource Manager machines to deliver applications and published desktops, you can choose a deployment method:

- **Full Configuration:** The Full Configuration option uses the Studio management console, which guides you through creating a machine catalog and then creating a Delivery Group. This deployment method offers advanced configuration features. This method can be used for any supported host type.
- **Azure Quick Deploy:** The Azure Quick Deploy option provides a simpler interface that offers faster deployment of apps and desktops. This deployment method offers basic configuration, without advanced features. This method is valid only when using Azure Resource Manager as your host.

Azure Quick Deploy offers a quick way to set up a proof of concept environment or to get started with Citrix Virtual Apps and Desktops service when using Azure Resource Manager.

If you are familiar with using Studio to deploy catalogs (either in on-premises Citrix Virtual Apps and Desktops, or Citrix Virtual Apps and Desktops service Full Configuration), there are some differences.

- Azure Quick Deploy uses different terminology: you create a catalog. In Full Configuration (Studio), you create a machine catalog.
- Azure Quick Deploy automatically creates server VMs and installs two Cloud Connectors in your resource location. In Full Configuration, these are separate steps you must complete before creating a catalog.
- Azure Quick Deploy does not use Delivery Groups. In Azure Quick Deploy, you configure all the deployment items in the catalog: the catalog, machines, applications, desktops, and subscribers. (A Delivery Group is automatically created for each Azure Quick Deploy catalog (using the same name as the catalog), but that action occurs behind the scenes. There is no required customer administrator action.)
- The Azure Quick Deploy interface has a different layout and style. There is more on-screen guidance.
The following graphic and table compare the deployment methods.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Azure Quick Deploy</th>
<th>Full Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploy to Azure</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deploy to Amazon Web Services and Google Cloud</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Deploy to on-premises hypervisors</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Deliver</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deliver Windows apps</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deliver multi-session OS desktops</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deliver Linux apps/desktops</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Deliver single session OS desktops</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User experience</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote PC Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Simplified user experience</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

If you are familiar with Citrix Virtual Apps Essentials service, the Azure Quick Deploy interface is very similar. It is easy to use, especially if you’re not familiar with Studio.

The deployment methods are not mutually exclusive. You can use one method to create some re-
sources, and then use the other method to create additional resources. However, where you edit a catalog can have effects; see Editing Azure Quick Deploy catalogs.

**Catalog displays**

Catalogs that are created using Azure Quick Deploy are visible in both the Azure Quick Deploy display and in Studio.

Machine catalogs that are created originally in Studio are not visible in the Azure Quick Deploy display.

**Limitations**

- Azure Quick Deploy is available only when using Azure Resource Manager as your host. It is not available with any other host types.
- Azure Quick Deploy is available only in the Citrix Virtual Apps and Desktops service and the Citrix Virtual Apps service. It is not offered in the Citrix Virtual Desktops service.
- Azure Quick Deploy delivers Windows multi-session OS machines. You cannot use it to deploy single session OS machines.
- You must be a full administrator to see both deployment options. If you are not a full admin, you won’t see the Azure Quick Deploy option, and will automatically use Full Configuration.
- See the Important note in editing Azure Quick Deploy catalogs.

**Citrix Gateway consideration**

If you use your own Citrix Gateway, it must have access to the VNET specified in the catalog creation wizard. A VPN can provide that access.

Alternatively, the Citrix Gateway Service works automatically with Azure Quick Deploy catalogs.

**Editing Azure Quick Deploy catalogs**

After you deploy a catalog using Azure Quick Deploy, it appears in the Quick Deploy Catalogs category on the Manage > Catalogs screen. You can use the ellipsis menu on a catalog’s row to select the following actions:

- Add or remove apps
- Add or remove subscribers
- Change capacity
- Select a different master image
- Delete the catalog
**Important:**
You can also use Studio to edit a catalog deployed with Azure Quick Deploy. However, if you use Studio to change that catalog or its corresponding Delivery Group, you will no longer be able to edit that catalog from the Azure Quick Deploy interface (Manage > Catalogs). The catalog will still be listed in Manage > Catalogs, but it can no longer be managed or deleted there.

**Use Azure Quick Deploy**

The Azure Quick Deploy sequence is essentially the same as the Citrix Virtual Apps Essentials service deployment interface.

Most of the guidance is available in the Citrix Virtual Apps Essentials service article. (In that article, disregard information about how to buy and cancel the service.)

1. Begin in the Create a catalog section, substituting the following procedure for step 2.
   - Click Catalogs (if it's not already selected). Select Manage > Azure Quick Deploy. Click Create a Catalog.

2. Follow the procedures for creating a catalog.

3. Follow the procedures for publishing apps and assigning subscribers for a catalog.

When you’ve successfully completed those steps, share the Workspace URL with your subscribers. For more information, see Launch applications and desktops.

**Create Delivery Groups**

June 3, 2019

**Introduction**

A Delivery Group is a collection of machines selected from one or more machine catalogs. The Delivery Group can also specify which users can use those machines, plus the applications and desktops available to those users.

Creating a Delivery Group is the next step in configuring your deployment after creating a machine catalog. Later, you can change the initial settings in the first Delivery Group and create other Delivery Groups. There are also features and settings you can configure only when editing a Delivery Group, not when creating it.

Before creating a Delivery Group:
Citrix Virtual Apps and Desktops service

- Review this section to learn about the choices you make and information you supply.
- Ensure that you have created a connection to the hypervisor, cloud service, other resource that hosts your machines.
- Ensure that you have created a machine catalog containing virtual or physical machines that will deliver apps and desktops.

To launch the Delivery Group creation wizard:

1. **Sign into Citrix Cloud.** In the upper left menu, select **My Services > Virtual Apps and Desktops**.
2. **Click Manage.**
3. If this is the first Delivery Group being created, the console guides you to the correct selection (such as “Set up delivery gorups to be displayed as services”). The Delivery Group creation wizard opens and walks you through the items described below.
4. If you already created a Delivery Group and want to create another, select **Delivery Groups** in the Studio navigation pane. Then select **Create Delivery Group** in the Actions pane.

The wizard walks you through the pages described below. The wizard pages you see may differ, depending on the selections you make.

**Step 1. Machines**

Select a machine catalog and select the number of machines you want to use from that catalog.

Good to know:

- At least one machine must remain unused in a selected catalog.
- A 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 machines from more than one 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. Similarly, if your deployment has catalogs of Windows machines and catalogs of Linux machines, a Delivery Group can contain machines from either OS type, but not both.
- Citrix recommends that you install or upgrade all VDAs with the latest version, and then upgrade machine catalogs and Delivery Groups as needed. When creating a Delivery Group, if you select machines that have different VDA versions installed, the Delivery Group will be compatible with the earliest VDA version. For example, if one of the machines you select has VDA version 7.1 installed and other machines have a later version, all machines in the group can use only those features that were supported in VDA 7.1. This means that some features that require newer VDA versions might not be available in that Delivery Group.
Step 2. Delivery type

This page appears only if you chose a machine catalog containing static (assigned) desktop OS machines. Choose either Applications or Desktops. You cannot enable both.

(If you selected machines from a server OS or desktop OS random (pooled) catalog, the delivery type is assumed to be applications and desktops. You can deliver applications, desktops, or both.)

Step 3. AppDisks

Ignore this page. Click Next.

Step 4. Users

Specify the users and user groups who can use the applications and desktops in the Delivery Group.

As an alternative to specifying applications in the Delivery Group wizard (as described in this section), you can configure them through the Citrix Cloud library.

Where user lists are specified

Active Directory user lists are specified when you create or edit the following:

- A deployment's user access list, which is not configured through this console. By default, the application entitlement policy rule includes everyone. See the PowerShell SDK BrokerAppEntitlementPolicyRule cmdlets for details.
- Delivery Groups.
- Applications.

The list of users who can access an application is formed by the intersection of the above user lists.

Authenticated and unauthenticated users

There are two types of users: authenticated and unauthenticated (unauthenticated is also called anonymous). You can configure one or both types in a Delivery Group.

- **Authenticated**: To access applications and desktops, 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 Workspace app. (For Delivery Groups containing desktop OS machines, you can import user data (a list of users) later by editing the Delivery Group.)
• **Unauthenticated (anonymous):** For Delivery Groups containing server OS machines, you can allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Workspace app. For example, at 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 first Delivery Controller.

To grant access to unauthenticated users, each machine in the Delivery Group must have a VDA for Windows Server OS 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 on the **Users** page:

<table>
<thead>
<tr>
<th>Enable access for</th>
<th>Add/assign users and user groups?</th>
<th>Enable the “Give access to unauthenticated users” check box?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only authenticated users</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Only unauthenticated users</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Both authenticated and unauthenticated users</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Step 5. Applications**

**Good to know:**

- You cannot add applications to Remote PC Access Delivery Groups.
- By default, new applications you add are placed in a folder named Applications. You can specify a different folder. For details, see the Applications article.
- You can change the properties for an application when you add it to a Delivery Group, or later. For details, see the Applications article.
- If you try to add an application and one with the same name already exists in that folder, you are prompted to rename the application you are adding. If you decline, the application is added with a suffix that makes it unique within that application folder.
- When you add an application to more than one Delivery Group, a visibility issue can occur if you do not have sufficient permission to view the application in all of those Delivery Groups. In such
cases, either consult an administrator with greater permissions or have your scope extended to include all the Delivery Groups to which the application was added.

- If you publish two applications with the same name to the same users, change the Application name (for user) property. Otherwise, users will see duplicate names in Citrix Workspace app.

Click the Add dropdown to display the application sources.

- **From Start menu:** Applications that are discovered on a machine created from the master image in the selected catalog. When you select this source, a new page launches with a list of discovered applications; select those you want to add and then click OK.

- **Manually defined:** Applications located in the deployment or elsewhere in your network. When you select this source, a new page launches where you type the path to the executable, working directory, optional command line arguments, and display names for administrators and users. After entering this information, click OK.

- **Existing:** Applications previously added to the deployment, perhaps in another Delivery Group. When you select this source, a new page launches with a list of discovered applications; select those you want to add and then click OK.

- **App-V:** Applications in App-V packages. When you select this source, a new page launches where you select the App-V server or the Application Library. Select the applications you want to add from the resulting display and then click OK.

If an application source or application is not available or valid, it is either not visible or cannot be selected. For example, the **Existing** source is not available if no applications have been added to the deployment. Or, an application might not be compatible with the supported session types on machines in the selected machine catalog.

As an alternative to specifying applications in the Delivery Group wizard (as described in this section), you can configure them through the Citrix Cloud library.

**Step 6. Desktops (or Desktop Assignment Rules)**

The title of this page depends on the machine catalog you chose earlier in the wizard:

- If you chose a catalog containing pooled machines, this page is titled **Desktops**.
- If you chose a catalog containing assigned machines and specified “Desktops” on the **Delivery Type** page, this page is titled **Desktop User Assignments**.
- If you chose a catalog containing assigned machines and specified “Applications” on the **Delivery Type** page, this page is titled **Application Machine User Assignments**.

Click **Add**. In the dialog box:

- In the **Display name** and **Description** fields, type the information to be displayed in Citrix Workspace app.
To add a tag restriction to a desktop, select **Restrict launches to machines with this tag** and then select the tag from the dropdown.

Using the radio buttons, indicate who can launch a desktop (for groups with pooled machines) or who will be assigned a machine when they launch the desktop (for groups with assigned machines). The users can be either everyone who can access this Delivery Group, or specific users and user groups.

If the group contains assigned machines, specify the maximum number of desktops per user. This must be a value of one or greater.

Enable or disable the desktop (for pooled machines) or desktop assignment rule (for assigned machines). Disabling a desktop stops desktop delivery; disabling a desktop assignment rule stops desktop auto-assignment to users.

When you are finished with the dialog box, click **OK**.

As an alternative to specifying desktops in the Delivery Group wizard (as described in this section), you can configure them through Citrix Cloud library.

### Step 7. Summary

Enter a name for the Delivery Group. You can also (optionally) enter a description, which will appear in Workspace app and in Studio.

Review the summary information and then click **Finish**. If you did not select any applications or specify any desktops to deliver, you are asked if you want to continue.

### If you don’t specify users or applications in the wizard

As an alternative to specifying users and applications in a Delivery Group, you can specify them in the Citrix Cloud console.

1. In the Citrix Cloud Console, select **Library**.

2. Find the card containing the resources (applications or desktops) you want. Hover over the ellipsis menu in the upper right corner and select **Manage Subscribers**.

3. In the **Manage subscribers** dialog, under **Add Subscribers** in the left dropdown, select subscribers (users). If you have multiple subscribers, you might need to type one or more characters of the domain group containing those users in the right search field. Matches appear in the table below the two fields. Select the correct match. (If there’s only one match, it’s automatically selected.) When the Status field indicates **Ready**, click the X in the upper right corner to close the dialog.

4. Refresh the **Resources** page. The lower left corner of the resource card contains a value that indicates domain users have been selected.
Here’s a video of this process.

More information

- Manage Delivery Groups
- Applications

Manage Delivery Groups

June 4, 2019

Introduction

This article describes procedures for managing Delivery Groups from the management console. In addition to changing settings specified when creating the group, you can configure other settings that are not available when you create a Delivery Group.
Citrix Virtual Apps and Desktops service

The procedures are organized by categories: general, users, machines, and sessions. Some tasks span more than one category. For example, “Prevent users from connecting to machines” is described in the machines category, but it also affects users. So, if you can’t find a task in one category, check a related category.

Other articles also contain related information:

• **Applications** contains information about managing applications in Delivery Groups.
• Managing Delivery Groups requires the Delivery Group Administrator built-in role permissions. For details, see [Delegated Administration](#).

**General**

• Change the delivery type
• Change StoreFront addresses
• Upgrade a Delivery Group
• Manage Remote PC Access Delivery Groups

**Change the delivery type of a Delivery Group**

The delivery type indicates what the group can deliver: applications, desktops, or both.

Before changing an **application only** or **desktops and applications** type to the **desktops only** type, delete all applications from the group.

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Delivery Type** page, select the delivery type you want.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

**Change StoreFront addresses**

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **StoreFront** page, select or add StoreFront URLs that are used by the Citrix Workspace app, which is installed on each machine in the Delivery Group.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

You can also specify StoreFront server addresses by selecting **Configuration > StoreFront** in the navigation pane.
Upgrade a Delivery Group or revert an upgrade

Upgrade a Delivery Group after you upgrade the VDAs on its machines and the machine catalogs containing the machines used in the Delivery Group.

Before you start the Delivery Group upgrade:

- If you use Citrix Provisioning (formerly Provisioning Services), upgrade the VDA version in the Citrix Provisioning console.
- Start the machines containing the upgraded VDA so that they can register with a Delivery Controller. This process tells the console about what needs upgrading in the Delivery Group.
- If you must continue to use earlier VDA versions, newer product features may not be available. For more information, see the upgrade documentation.

To upgrade a Delivery Group:

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Upgrade Delivery Group** in the Actions pane. The **Upgrade Delivery Group** action appears only if upgraded VDAs are detected.

The display indicates you which, if any, machines cannot be upgraded and why. You can then cancel the upgrade, resolve the machine issues, and then start the upgrade again.

After the upgrade completes, you can revert the machines to their previous states by selecting the Delivery Group and then clicking **Undo** in the Actions pane.

Manage Remote PC Access Delivery Groups

If a machine in a Remote PC Access machine catalog is not assigned to a user, the machine is temporarily assigned to a Delivery Group associated with that catalog. This temporary assignment enables the machine to be assigned to a user later.

The Delivery Group-to-machine catalog association has a priority value. Priority determines which Delivery Group that machine is assigned to 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. Use the PowerShell SDK to set this priority value.

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 catalog later can be added to the Delivery Group. This association can be switched off or on.

To add or remove a Remote PC Access machine catalog association with a Delivery Group:

1. Select **Delivery Groups** in the navigation pane.
2. Select a Remote PC PC Access group.
3. In the **Details** section, click the **Machine Catalogs** tab and then select a Remote PC Access catalog.
4. To add or restore an association, click **Add Desktops**. To remove an association, click **Remove Association**.

**Users**

- Change user settings
- Add or remove users

**Change user settings in a Delivery Group**

The name of this page appears as either **User Settings** or **Basic Settings**.

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **User Settings** (or **Basic Settings**) page, change any of the settings in the following table.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The text that Citrix Workspace (or StoreFront) uses and that users see.</td>
</tr>
<tr>
<td>Enable Delivery Group</td>
<td>Whether the Delivery Group is enabled.</td>
</tr>
<tr>
<td>Time zone</td>
<td></td>
</tr>
<tr>
<td>Enable Secure ICA</td>
<td>Secures communications to and from machines in the Delivery Group using SecureICA, which encrypts the ICA protocol. The default level is 128-bit. The level can be changed using the SDK. Citrix recommends using additional encryption methods such as TLS encryption when traversing public networks. Also, SecureICA does not check data integrity.</td>
</tr>
</tbody>
</table>
Add or remove users in a Delivery Group

For detailed information about users, see Users.

1. Select Delivery Groups in the navigation pane.
2. Select a group and then click Edit Delivery Group in the Actions pane.
3. On the Users page:
   • To add users, click Add, and then specify the users you want to add.
   • To remove users, select one or more users and then click Remove.
   • Select or clear the checkbox to allow access by unauthenticated users.
4. Click Apply to apply any changes you made and keep the window open. Or, click OK to apply changes and close the window.

Import or export user lists

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 navigation pane.
2. Select a group and then click Edit Delivery Group in the Actions pane.
3. On the Machine Allocation page, select Import list or Export list, and then browse to the file location.
4. Click Apply to apply any changes you made and keep the window open. Or, click OK to apply changes and close the window.

Machines

- Change assignments of machines to users
- Change the maximum number of machines per user
- Update a machine
- Add, change, or remove a tag restriction for a desktop
- Remove a machine
- Restrict access to machines
Citrix Virtual Apps and Desktops service

- Prevent users from connecting to a machine (maintenance mode)
- Shut down and restart machines
- Create and manage restart schedules for machines
- Load manage machines

In addition to the features described in this article, see Autoscale for information about proactively power managing machines.

**Change assignments of machines to users in a Delivery Group**

You can change the assignments of desktop OS machines provisioned with MCS. You cannot change assignments for server OS machines or machines provisioned with Citrix Provisioning.

1. Select Delivery Groups in the navigation pane.
2. Select a group and then click Edit Delivery Group in the Actions pane.
3. On the Desktops or Desktop Assignment Rules page (the page title depends on the type of machine catalog the Delivery Group uses), specify the new users.
4. Click Apply to apply any changes you made and keep the window open. Or, click OK to apply changes and close the window.

**Change the maximum number of machines per user in a Delivery Group**

1. Select Delivery Groups in the navigation pane.
2. Select a group and then click Edit Delivery Group in the Actions pane.
3. On the Desktop Assignment Rules page, set the maximum desktops per user value.
4. Click Apply to apply any changes you made and keep the window open. Or, click OK to apply changes and close the window.

**Update a machine in a Delivery Group**

1. Select Delivery Groups in the navigation pane.
2. Select a group and then click View Machines in the Actions pane.
3. Select a machine and then click Update Machines in the Actions pane.

To choose a different master image, select Master image and then select a snapshot.

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 (the total time to begin updating all machines in the group)
- Whether users are notified of the restart
- The message users will receive
Add, change, or remove a tag restriction for a desktop

Adding, changing, and removing tag restrictions can have unanticipated effects on which desktops are considered for launch. Review the considerations and cautions in Tags.

1. Select Delivery Groups in the navigation pane.
2. Select a group and then click Edit Delivery Group in the Actions pane.
3. On the Desktops page, select the desktop and click Edit.
4. To add a tag restriction, select Restrict launches to machines with the tag and then select the tag.
5. To change or remove a tag restriction, either:
   - Select a different tag.
   - Remove the tag restriction by clearing Restrict launches to machines with this tag.
6. Click Apply to apply any changes you made and keep the window open. Or, click OK to apply changes and close the window.

Remove a machine from a Delivery Group

Removing a machine deletes it from a Delivery Group. It does not delete it from the machine catalog that the Delivery Group uses. Therefore, that machine is available for assignment to another Delivery Group.

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.

Machines might contain personal data, so use caution before allocating the machine to another user. Consider reimaging the machine.

1. Select Delivery Groups in the navigation pane.
2. Select a group and then click View Machines in the Actions pane.
3. Ensure that the machine is shut down.
4. Select the machine and then click Remove from Delivery Group in the Actions pane.

You can also remove a machine from a Delivery Group through the connection the machine uses.

Restrict access to machines in a Delivery Group

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. For details, see [Delegated Administration](#).

- **Restrict access for users through SmartAccess policy expressions:** Use policy expressions to filter user connections made through Citrix Gateway.
  1. Select **Delivery Groups** in the navigation pane.
  2. Select a group and then click **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 Citrix Gateway site, and add, edit, or remove the SmartAccess policy expressions for the allowed user access scenarios. For details, see the Citrix Gateway documentation.
  5. Click **Apply** to apply any changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

- **Restrict access for users through exclusion filters:** Use 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 corporate network subnet, to prevent access from that lab to a particular Delivery Group, regardless of who is using the machines in the lab, use the command: 
  ```powershell
  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.

  If you are connected using a web browser or with the Citrix Workspace app user experience feature enabled in the store, you cannot use a client name exclusion filter.

### Prevent users from connecting to a machine (maintenance mode) in a Delivery Group

When you need to temporarily stop new connections to machines, you can turn on maintenance mode for one or all 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.
Citrix Virtual Apps and Desktops service

- 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.

To turn maintenance mode on or off:

1. Select **Delivery Groups** in the navigation pane.
2. Select a group.
3. To turn on maintenance mode for all machines in the Delivery Group, click **Turn On Maintenance Mode** in the Actions pane.

   To turn on maintenance mode for one machine, click **View Machines** in the Actions pane. Select a machine, and then click **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 click **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:

- 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 either **Allow reconnections, but prevent new logons** or **Allow reconnections, but prevent new logons until the server is restarted**.

You can also turn maintenance mode on or off for:

- A connection, which affects the machines using that connection.
- A machine catalog, which affects the machines in that catalog.

**Shut down and restart machines in a Delivery Group**

This procedure is not supported for Remote PC Access machines.

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **View Machines** in the Actions pane.
3. Select the machine and then click one of the following entries 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.
   - **Force restart**: Forcibly shuts down the operating system and then restarts the machine.
Citrix Virtual Apps and Desktops service

- **Suspend:** Pauses the machine without shutting it down, and refreshes the list of machines.
- **Shut down:** Requests the operating system to shut down.

For non-force actions, 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.

Citrix recommends that you prevent desktop OS machine users from selecting **Shut down** within a session. See the Microsoft policy documentation for details.

You can also shut down and restart machines on a connection.

**Create and manage restart schedules for machines in a Delivery Group**

A restart schedule specifies when machines in a Delivery Group are periodically restarted. You can create one or more schedules for a Delivery Group. A schedule can affect either:

- All of the machines in the group.
- One or more (but not all) machines in the group. The machines are identified by a tag that you apply to the machine. This is called a tag restriction, because the tag restricts an action to only items (in this case, machines) that have the tag.

For example, let’s say all of your machines are in one Delivery Group. You want every machine restarted once every week, and you want the machines used by the accounting team restarted daily. To accomplish this, set up one schedule for all machines, and another schedule for only the machines in accounting.

A schedule includes the day and time the restart begins, and the duration. The duration is either “start all affected machines at the same time” or an interval it should take to restart all affected machines.

You can enable or disable a schedule. Disabling a schedule can be helpful when testing, during special intervals, or when preparing schedules before you need them.

You cannot use schedules for automated power-on or shutdown from the management console, only to restart.

**Schedule overlap**

Multiple schedules can overlap. In the example above, both schedules affect the accounting machines. Those machines might be restarted twice on Sunday. The scheduling code is designed to avoid restarting the same machine more often than intended, but it cannot be guaranteed.

- If the schedules coincide precisely in start and duration times, it is more likely that the machines will be restarted only once.
The more the schedules differ in start and duration times, it’s more likely that multiple restarts will occur.

The number of machines affected by a schedule also affects the chance of an overlap. In the example, the weekly schedule that affects all machines might initiate restarts significantly faster than the daily schedule for accounting machines, depending on the duration specified for each.

For an in-depth look at restart schedules, see Reboot schedule internals.

View restart schedules

1. Select Delivery Groups in the navigation pane.
2. Select a group and then click Edit Delivery Group in the Actions pane.
3. Select the Restart Schedule page.

The Restart Schedule page contains the following information for each configured schedule:

- Schedule name.
- Tag restriction used, if any.
- How often the machine restarts occur.
- Whether machine users receive a notification.
- Whether the schedule is enabled. Disabling a schedule can be helpful when testing, during special intervals, or when preparing schedules before you need them.

Add (apply) tags

When you configure a restart schedule that uses a tag restriction, ensure that the tag has been added (applied) to the machines that the schedule affects. In the example above, each of the machines used by the accounting team has a tag applied. For details, see Tags.

Although you can apply more than one tag to a machine, a restart schedule can specify only one tag.

1. Select Delivery Groups in the navigation pane.
2. Select the group containing the machines to be controlled by the schedule.
3. Click View Machines and then select the machines you want to add a tag to.
4. Click Manage Tags in the Actions pane.
5. If the tag exists, enable the check box next to the tag name. If the tag does not exist, click Create and then specify the name for the tag. After the tag is created, enable the check box next to the newly created tag name.
6. Click Save in the Manage Tags dialog.

Create a restart schedule

1. Select Delivery Groups in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.

3. On the **Restart Schedule** page, click **Add**.

4. On the **Add Restart Schedule** page:
   - Type a schedule name and description.
   - If you’re using a tag restriction, select the tag.
   - In **Restart frequency**, select how often the restart occurs: daily, weekdays, weekend days, or a specific day each week.
   - Using the 24-hour clock, specify the time of day to begin the restart.
   - For **Restart duration**, choose whether all machines should be restarted at the same time, or the total length of time to begin restarting all of the affected machines. An internal algorithm determines when each machine is restarted during that interval.
   - In **Send notification to users**, choose whether to display a notification message on the affected machines before a restart begins. By default, no message is displayed.
   - If you choose to display a message 15 minutes before the restart begins, you can choose (in **Notification frequency**) to repeat the message every five minutes after the initial message. By default, the message is not repeated.
   - Enter the notification title and text. There is no default text.
     
     If you want the message to include the number of minutes before restart, include the variable %m%. For example: “Warning: Your computer is automatically restarted in %m% minutes.” The value decrements by five minutes in each repeated message. Unless you chose to restart all machines at the same time, the message displays on each machine at the appropriate time before the restart, calculated by the internal algorithm.
   - To enable the schedule, select the check box. To disable the schedule, clear the check box.

5. Click **Apply** to apply changes you made and keep the window open. Or, click **OK** to apply changes and close the window.

**Edit, remove, enable, or disable a restart schedule**

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Restart Schedule** page, select the check box for a schedule.
   - To edit a schedule, click **Edit**. Update the schedule configuration, using the guidance in Create a restart schedule.
   - To enable or disable a schedule, click **Edit**. Select or clear the **Enable restart schedule** check box.
To remove a schedule, click **Remove**. Confirm the removal. Removing a schedule does not affect any tags applied to machines in the affected machines.

**Load manage machines in Delivery Groups**

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.
- **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. Load evaluators are specified in load management policy settings.

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.

You can monitor the load index in Director (Monitor), Studio (Manage) search, and the SDK.

In console displays, to display the **Server Load Index** column (which is hidden by default), select a machine, right-click a column heading, and then select **Select Column**. In the **Machine category**, select **Load Index**.

In the SDK, use the `Get-BrokerMachine` cmdlet. For details, see [CTX202150](#).

- **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 6.x versions.)

When 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 these criteria, the server with the lowest load index is selected.

**Sessions**

- Log off or disconnect a session, or send a message to users
- Configure session prelaunch and session linger

**Log off or disconnect a session, or send a message to Delivery Group users**

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **View Machines** in the Actions pane.

3. To log a user off a session, select the session or desktop and then click **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.

4. To disconnect a session, select the session or desktop and then click **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.

5. To send a message to users, select the session, machine, or user and then click **Send message** in the Actions pane. Enter the message.

### Configure session prelaunch and session linger in a Delivery Group

These features are supported only on server OS machines.

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.
- These features are supported only when using Citrix Workspace app for Windows, and also require additional Citrix Workspace app configuration. For instructions, search for session prelaunch in the product documentation for your Citrix Workspace app for Windows version.
- Citrix Workspace app for HTML5 is not supported.
- When using session prelaunch, if a user’s machine is put into suspend or hibernate mode, prelaunch does not work (regardless of session prelaunch settings). Users can lock their machines/sessions. However, if a user logs off from Citrix Workspace app, the session is ended and prelaunch no longer applies.
- When using session prelaunch, physical client machines cannot use the suspend or hibernate power management functions. Client machine users can lock their sessions but should not log off.
- Prelaunched and lingering sessions consume a concurrent license, but only when connected. If using a user/device license, the license lasts 90 days. 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 appli-
cation 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 Citrix Workspace app.

**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 causes 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 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 can enable this timeout from the SDK only (New/Set-BrokerSessionPreLaunch cmdlet), not from the management console. If you disable the timeout, it does not appear in the console display for that Delivery Group or in the **Edit Delivery Group** pages.

- **Thresholds:** Automatically ending prelaunched and lingering sessions based on server load ensures that sessions remain open as long as possible, assuming that server resources are available. Unused prelaunched and lingering sessions do not cause denied connections because they are 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 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 a Controller and servers in maintenance mode are considered fully loaded. An unplanned outage causes prelaunch and lingering sessions to end automatically to free capacity.

**To enable session prelaunch**

1. Select **Delivery Groups** in the navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Application Prelaunch** page, enable session prelaunch by choosing when sessions 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 Citrix Workspace app for Windows.
• When anyone in a list of users and user groups logs on to Citrix Workspace app 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.

• 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 navigation pane.
2. Select a group and then click Edit Delivery Group in the Actions pane.
3. On the Application Lingering page, enable session linger by selecting Keep sessions active until.
4. Several settings affect how long a lingering session remains active if the user does not start another application.

• 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.

Troubleshoot

• VDAs that are not registered with a Delivery Controller are not considered when launching brokered sessions. This results in underutilization of otherwise available resources. There are various reasons a VDA might not be registered, many of which an administrator can troubleshoot.
The details display provides troubleshooting information in the catalog creation wizard, and after you add a catalog to a Delivery Group.

After you create a Delivery Group, the details pane for a Delivery Group indicates the number of machines that should be registered but are not. For example, one or more machines are powered on and not in maintenance mode, but are not currently registered with a Controller. When viewing a “not registered, but should be” machine, review the **Troubleshoot** tab in the details pane for possible causes and recommended corrective actions.

For messages about functional level, see [VDA versions and functional levels](#).

For information about VDA registration troubleshooting, see [CTX136668](#).

- In the display for a Delivery Group, the **Installed VDA version** in the details pane might differ from the actual version installed on the machines. The machine’s Windows Programs and Features display shows the actual VDA version.

- For machines with **Power State Unknown** status, see [CTX131267](#) for guidance.

## Create Application Groups

**August 21, 2019**

### Introduction

Application Groups let you manage collections of applications. You can create Application Groups for applications shared across different Delivery Groups or used by a subset of users within Delivery Groups. Application Groups are optional; they offer an alternative to adding the same applications to multiple Delivery Groups. Delivery Groups can be associated with more than one Application Group, and an Application Group can be associated with more than one Delivery Group.

Using Application Groups can provide application management and resource control advantages over using more Delivery Groups:

- The logical grouping of applications and their settings lets you manage those applications as a single unit. For example, you don’t have to add (publish) the same application to individual Delivery Groups one at a time.
- Session sharing between Application Groups can conserve resource consumption. In other cases, disabling session sharing between Application Groups may be beneficial.
- You can use the tag restriction feature to publish applications from an Application Group, considering only a subset of the machines in selected Delivery Groups. With tag restrictions, you can use your existing machines for more than one publishing task, saving the costs associated with
deploying and managing additional machines. A tag restriction can be thought of as subdivid-
ing (or partitioning) the machines in a Delivery Group. Using an Application Group or desktops
with a tag restriction can be helpful when isolating and troubleshooting a subset of machines
in a Delivery Group.

Example configurations

Example 1

The following graphic shows a deployment that includes Application Groups:

In this configuration, applications are added to the Application Groups, not the Delivery Groups. The
Delivery Groups specify which machines will be used. (Although not shown, the machines are in ma-
icine catalogs.)

Application Group 1 is associated with Delivery Group 1. The applications in Application Group 1 can
be accessed by the users specified in Application Group 1, as long as they are also in the user list for
Delivery Group 1. This follows the guidance that the user list for an Application Group should be a
subset (a restriction) of the user lists for the associated Delivery Groups. The settings in Application
Group 1 (such as application session sharing between Application Groups, associated Delivery Groups)
apply to applications and users in that group. The settings in Delivery Group 1 (such as anonymous
user support) apply to users in Application Groups 1 and 2, because those Application Groups have
been associated with that Delivery Group.

Application Group 2 is associated with two Delivery Groups: 1 and 2. Each of those Delivery Groups can
be assigned a priority in Application Group 2, which indicates the order in which the Delivery Groups
will be checked when an application is launched. Delivery Groups with equal priority are load bal-
anced. The applications in Application Group 2 can be accessed by the users specified in Application
Group 2, as long as they are also in the user lists for Delivery Group 1 and Delivery Group 2.

Example 2

This simple layout uses tag restrictions to limit which machines will be considered for certain desktop
and application launches. The site has one shared Delivery Group, one published desktop, and one
Application Group configured with two applications.

Tags have been added to each of the three machines (VDA 101-103).

The Application Group was created with the “Orange” tag restriction, so each of its applications (Cal-
culator and Notepad) can be launched only on machines in that Delivery Group that have the tag
“Orange”: VDA 102 and 103.

For more comprehensive examples and guidance for using tag restrictions in Application Groups (and
for desktops), see Tags.
Guidance and considerations

Citrix recommends adding applications to either Application Groups or Delivery Groups, but not both. Otherwise, the additional complexity of having applications in two group types can make it more difficult to manage.

By default, an Application Group is enabled. After you create an Application Group, you can edit the group to change this setting. See Manage Application Groups.

By default, application session sharing between Application Groups is enabled. See Session sharing between Application Groups.

Citrix recommends that your Delivery Groups be upgraded to the current version. This requires:

1. Upgrading VDAs on the machines used in the Delivery Group
2. Upgrading the machine catalogs containing those machines
3. Upgrading the Delivery Group.

For details, see Manage Delivery Groups.

To use Application Groups, your core components must be minimum version 7.9.

Creating Application Groups requires the Delegated Administration permission of the Delivery Group Administrator built-in role. See Delegated Administration for details.

This article refers to “associating” an application with more than one Application Group to differentiate that action from adding a new instance of that application from an available source. Similarly, Delivery Groups are associated with Application Groups (and vice versa), rather than being additions or components of one another.

Session sharing with Application Groups

When application session sharing is enabled, all applications launch in the same application session. This saves the costs associated with launching additional application sessions, and allows the use of application features that involve the clipboard, such as copy-paste operations. However, in some situations you may wish to turn off session sharing.

When you use Application Groups you can configure application session sharing in the following three ways which extend the standard session sharing behavior available when you are using only Delivery Groups:

- Session sharing enabled between Application Groups.
- Session sharing enabled only between applications in the same Application Group.
- Session sharing disabled.
**Session sharing between Application Groups**

You can enable application session sharing between Application Groups, or you can disable it to limit application session sharing only to applications in the same Application Group.

- **An example when enabling session sharing between Application Groups is helpful:**
  Application Group 1 contains Microsoft Office applications such as Word and Excel. Application Group 2 contains other applications such as Notepad and Calculator, and both Application Groups are attached to the same Delivery Group. A user who has access to both Application Groups starts an application session by launching Word, and then launches Notepad. If the user's existing session running Word is suitable for running Notepad then Notepad is started within the existing session. If Notepad cannot be run from the existing session—for example if the tag restriction excludes the machine that the session is running on—then a new session on a suitable machine is created rather than using session sharing.

- **An example when disabling session sharing between Application Groups is helpful:**
  You have a set of applications that do not interoperate well with other applications that are installed on the same machines, such as two different versions of the same software suite or two different versions of the same web browser. You prefer not to allow a user to launch both versions in the same session.

  You create an Application Group for each version of the software suite, and add the applications for each version of the software suite to the corresponding Application Group. If session sharing between groups is disabled for each of those Application Groups, a user specified in those groups can run applications of the same version in the same session, and can still run other applications at the same time, but not in the same session. If the user launches one of the different-versioned applications (that are in a different Application Group), or launches any application that is not contained in an Application Group, then that application is launched in a new session.

This session sharing between Application Groups feature is not a security sandboxing feature. It is not foolproof, and it cannot prevent users from launching applications into their sessions through other means (for example, through Windows Explorer).

If a machine is at capacity, new sessions are not started on it. New applications are started in existing sessions on the machine as needed using session sharing (providing that this complies with the session sharing restrictions described here).

You can only make prelaunched sessions available to Application Groups which have application session sharing allowed. (Sessions which use the session linger feature are available to all Application Groups.) These features must be enabled and configured in each of the Delivery Groups associated with the Application Group. You cannot configure them in the Application Groups.
Citrix Virtual Apps and Desktops service

By default, application session sharing between Application Groups is enabled when you create an Application Group. You cannot change this when you create the group. After you create an Application Group, you can edit the group to change this setting. See Manage Application Groups.

Disable session sharing within an Application Group

You can prevent application session sharing between applications which are in the same Application Group.

- An example when disabling session sharing within Application Groups is helpful:

  You want your users to access multiple simultaneous full screen sessions of an application on separate monitors.

  You create an Application Group and add the applications to it. If session sharing is prohibited between applications in that Application Group, when a user specified in it starts one application after another they launch in separate sessions, and the user can move each to a separate monitor.

By default, application session sharing is enabled when you create an Application Group. You cannot change this when you create the group. After you create an Application Group, you can edit the group to change this setting. See Manage Application Groups.

Create an Application Group

To create an Application Group:

1. Select Applications in the Studio navigation pane, and then select Create Application Group in the Actions pane.
2. The Create Application Group wizard launches with an Introduction page, which you can remove from future launches of this wizard.
3. The wizard guides you through the pages described below. When you are done with each page, click Next until you reach the Summary page.

Step 1. Delivery Groups

The Delivery Groups page lists all Delivery Groups, with the number of machines each group contains.

- The Compatible Delivery Groups list contains Delivery Groups you can select. Compatible Delivery Groups contain random (not permanently or statically assigned) server or desktop OS machines.
- The Incompatible Delivery Groups list contains Delivery Groups you cannot select. Each entry explains why it is not compatible, such as containing static assigned machines.
An Application Group can be associated with Delivery Groups containing shared (not private) machines that can deliver applications.

You can also select Delivery Groups containing shared machines that deliver only desktops, if both of the following conditions are met:

- The Delivery Group contains shared machines and was created with a XenDesktop version earlier than 7.9.
- You have Edit Delivery Group permission.

The Delivery Group type is automatically converted to “desktops and applications” when the Create Application Group wizard is committed.

Although you can create an Application Group that has no associated Delivery Groups (perhaps to organize applications or to serve as storage for applications not currently used) the Application Group cannot be used to deliver applications until it specifies at least one Delivery Group. Additionally, you cannot add applications to the Application Group from the From Start menu source if there are no Delivery Groups specified.

The Delivery Groups you select specify the machines that will be used to deliver applications. Select the check boxes next to the Delivery Groups you want to associate with the Application Group.

To add a tag restriction, select **Restrict launches to machines with the tag** and then select the tag from the dropdown.

**Step 2. Users**

Specify who can use the applications in the Application Group. You can either allow all users and user groups in the Delivery Groups you selected on the previous page, or select specific users and user groups from those Delivery Groups. If you restrict use to users you specify, then only the users specified in the Delivery Group and the Application Group can access the applications in this Application Group. Essentially, the user list in the Application Group provides a filter on the user lists in the Delivery Groups.

Enabling or disabling application use by unauthenticated users is available only in Delivery Groups, not in Application Groups.

For information about where user lists are specified in a deployment, see [Where user lists are specified](#).

**Step 3. Applications**

Good to know:
• By default, new applications you add are placed in a folder named Applications. You can specify a different folder. If you try to add an application and one with the same name already exists in that folder, you are prompted to rename the application you are adding. If you agree with the suggested unique name, the application is added with that new name. Otherwise, you must rename it yourself before it can be added. For details, see Manage application folders.

• You can change an application’s properties (settings) when you add it, or later. See Change application properties. 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 Citrix Workspace app.

• When you add an application to more than one Application Group, a visibility issue can occur if you do not have sufficient permission to view the application in all of those groups. In such cases, either consult an administrator with greater permissions or have your scope extended to include all the groups to which the application was added.

Click the Add dropdown to display the application sources.

• From Start menu: Applications that are discovered on a machine in the selected Delivery Groups. When you select this source, a new page launches with a list of discovered applications. Select the check boxes of applications to add, and then click OK.

This source cannot be selected if you selected any of the following:

– Application Groups that have no associated Delivery Groups.
– Application Groups with associated Delivery Groups that contain no machines.
– A Delivery Group containing no machines.

• Manually defined: Applications located in the Site or elsewhere in your network. When you select this source, a new page launches where you type the path to the executable, working directory, optional command line arguments, and display names for administrators and users. After entering this information, click OK.

• Existing: Applications previously added to the Site. When you select this source, a new page launches with a list of discovered applications. Select the check boxes of applications to add and then click OK. This source cannot be selected if the Site has no applications.

• App-V: Applications in App-V packages. When you select this source, a new page launches where you select the App-V server or the Application Library. From the resulting display, select the checkboxes of applications to add, and then click OK. For more information, see App-V. This source cannot be selected (or might not appear) if App-V is not configured for the Site.

As noted, certain entries in the Add dropdown will not be selectable if there is no valid source of that type. Sources that are incompatible are not listed at all (for example, you cannot add Application Groups to Application Groups, so that source is not listed when you create an Application Group).
Step 4. Scopes

This page appears only if you have previously created a custom scope. By default, the All scope is selected. For more information, see Delegated Administration.

Step 5. Summary

Enter a name for the Application Group. You can also (optionally) enter a description.

Review the summary information and then click Finish.

Remove components

August 29, 2018

To remove components that you installed (such as VDAs), Citrix recommends using the Windows feature for removing or changing programs. Alternatively, you can remove components using the command line, or a script.

When you remove components, prerequisites are not removed, and firewall settings are not changed.

When you remove a VDA, the machine restarts automatically after the removal, by default.

Remove components using the Windows feature for removing or changing programs

From the Windows feature for removing or changing programs:

- 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.

Remove a VDA using the command line

Run the command that was used to install the VDA: VDAServerSetup.exe, VDAWorkstationSetup.exe, or VDAWorkstationCoreSetup.exe. See Install using the command line for syntax descriptions.

- To remove only the VDA or only the Citrix Workspace app, use the /remove and /components options.
- To remove the VDA and Citrix Workspace app, use the /removeall option.
For example, the following command removes the VDA and Citrix Workspace app from a server OS machine.

`VDAServerSetup.exe /removeall`

For example, the following command removes the VDA but not Citrix Workspace app for Windows (if it is installed) from a desktop OS machine.

`VDAWorkstationSetup.exe /remove /component vda`

You can also remove a VDA using a script provided by Citrix. See Remove VDAs using the script.

**Upgrade**

April 25, 2019

Citrix maintains all of the core Citrix Virtual Apps and Desktops service components in your deployment, except VDAs.

To upgrade a VDA, download the installer (as you did when you originally installed it) and run it on the machine or image. You can use the installer’s graphical or command-line interface.

If you originally installed the VDA using `VDAWorkstationCoreSetup.exe`, you will retain that configuration if you upgrade it with the latest version of the same installer. If you run `VDAWorkstationSetup.exe` on that machine, you can enable the features that are not supported in the `VDAWorkstationCoreSetup.exe` installer. (Keep in mind that some of those features might be enabled by default in the `VDAWorkstationSetup.exe` installer.) Additionally, you will have the option to install Citrix Workspace app.

When upgrading a VDA to version 7.17 or a later supported version, a machine restart occurs during the upgrade process. This cannot be avoided. The upgrade resumes automatically after the restart (unless you specify `/noresume` on the command line).

After you upgrade VDAs, update the master images and catalogs that use that VDA.

Learn about product name changes.

**Earlier operating systems**

For machines with OSs that are no longer supported for installation of the latest VDA (such as Windows 7 and Windows Server 2008 R2), you have several options.

- Reimage the machine to a supported Windows version, and then install the new VDA.
• If reimaging the machine is not an option but you want to upgrade the OS, uninstall the VDA before upgrading the OS. Otherwise, the VDA will be in an unsupported state. Then, install the new VDA.
• If you want to continue to use machines with an OS that is no longer supported for VDA 7.16 or later, XenApp and XenDesktop 7.15 LTSR is the most current supported VDA version for Windows 7 and Windows Server 2008 R2.
  – If the machine has version 7.15 LTSR installed (and you attempt to install a newer version), a message informs you that you’re using the latest supported version.
  – If the machine has a version earlier than 7.15 LTSR installed, a message guides you to CTX139030 for information. You can download 7.15 LTSR VDAs from the Citrix web site.

More information

• Install VDAs
• Install VDAs using the command line
• Manage machine catalogs

Print

August 29, 2018

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.

For complete information about printing in a Citrix Virtual Apps and Desktops environment, begin with Print. From that article, you can move on to:

• Printing configuration examples
• Best practices

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Citrix Virtual Apps and Desktops service

- Printing policies and preferences
- Provision printers
- Maintain the printing environment

Install the Universal Print Server on your print servers

1. Ensure that each print server has Microsoft Virtual C++ Runtime 2013, 32-bit and 64-bit installed.
2. Navigate to the Citrix Universal Print Server download page and click Download File.
3. Run one of the following commands on each print server:
   - For a 32-bit operating system: `UpsServer_x86.msi`.
   - For a 64-bit operating system: `UpsServer_x64.msi`.

After you install the Universal Print Server, configure it using the guidance in Provision printers.

HDX technologies

August 29, 2018

Citrix HDX offers a broad set of technologies that provide a high-definition user experience at the device, on the network, and in the datacenter. For details, see the articles in the following categories:

- HDX
- Devices
- Graphics
- Multimedia
- Content redirection

Policies

August 29, 2018

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.
Citrix Virtual Apps and Desktops service

For complete information about Citrix policies, begin with Policies. From that article, you can move on to:

- Work with policies
- Policy templates
- Create policies
- Compare, prioritize, model, and troubleshoot policies
- Default policy settings
- Policy settings reference

Manage

June 19, 2019

Citrix manages Citrix Virtual Apps and Desktops service deployments by installing and maintaining the core components and features in Citrix Cloud. You take care of the machines (VDAs) in resource locations that deliver apps and desktops. You also manage connections to those resource locations, as well as the apps, desktops, and users.

- **Applications**: Manage applications in Delivery Groups.
- **Virtual IP and virtual loopback**: 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.*).
- **VDA registration**: Before a VDA can facilitate delivery of apps and desktops, it must register (establish communication) with a Cloud Connector. You can specify Cloud Connector addresses using several methods, which are described in this article. VDAs must have current information as you add Cloud Connectors.
- **Sessions**: Maintaining session activity is critical to providing the best user experience. Several features can optimize the reliability of sessions, reduce inconvenience, downtime, and loss of productivity.
- **Using Search**: To view information about machines, sessions, machine catalogs, applications, or Delivery Groups in Studio, use the flexible search feature.
- **IPv4/IPv6 support**: Citrix Virtual Apps and Desktops supports pure IPv4, pure IPv6, and dual-stack deployments that use overlapping IPv4 and IPv6 networks. This article describes and illustrates these deployments. It also describes the Citrix policy settings that control the use of IPv4 or IPv6.
Citrix Virtual Apps and Desktops service

- **Profile management**: Citrix Profile management can be installed when you install a VDA. If you use this user profile solution, review its documentation.

- **Citrix Insight Services**: Citrix Insight Services (CIS) is a Citrix platform for instrumentation, telemetry, and business insight generation. Analytics and diagnostics are collected when you install a VDA.

- **Local Host Cache**: Local Host Cache enables connection brokering operations to continue when a Cloud Connector in a resource location cannot communicate with Citrix Cloud.

- **Delegated Administration**: With Delegated Administration, you can configure the access permissions that all of your administrators need, in accordance with their role in your organization.

- **Configuration Logging**: Configuration Logging allows administrators to keep track of configuration changes and administrative activities.

- **Event logs**: Services within Citrix Virtual Apps and Desktops log events that occur. Event logs can be used to monitor and troubleshoot operations.

**Autoscale**

October 8, 2019

Autoscale is a feature exclusive to Citrix Virtual Apps and Desktops service that provides a consistent, high-performance solution to proactively power manage your machines. It aims to balance costs and user experience. Autoscale incorporates the deprecated Smart Scale technology into the Studio power management solution.

**About Autoscale**

Autoscale enables proactive power management of all registered Server and Desktop OS machines in a Delivery Group.

**Supported VDA hosting platforms**

Autoscale supports all the platforms that Virtual Apps and Desktops service supports. This includes a variety of infrastructure platforms including Citrix Hypervisor, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere, and many more. For a complete list of supported platforms, see System requirements for Virtual Apps and Desktops service.
**Supported workloads**

Autoscale works with both Remote Desktop Service (RDS) and Virtual Desktop Infrastructure (VDI). There are three user interfaces to be aware of:

- Autoscale user interface for RDS Delivery Groups
- Autoscale user interface for pooled VDI Delivery Groups
- Autoscale user interface for static VDI Delivery Groups

For more information about the user interfaces for different Delivery Groups, see *Three types of Autoscale user interfaces*.

**Benefits**

The Autoscale feature delivers the following benefits:

- Provide you with a single, consistent mechanism to power manage machines in a Delivery Group.
- Ensure availability and control costs by powering machines with load-based or schedule-based power management, or a combination of both.
- To monitor metrics such as cost savings and capacity utilization, and to enable notifications, use *Director*, available on the *Monitor* tab.

**Watch a 2-minute video**

The following video provides a quick tour of Autoscale.
Migration

Migration from Smart Scale to Autoscale is supported. Migrating includes exporting configuration data from Smart Scale and then importing it to Autoscale. For more information, see Smart Scale to Autoscale migration.

Three types of Autoscale user interfaces

There are three types of Autoscale user interfaces to be aware of. See below for details.

Autoscale user interface for RDS Delivery Groups:
Autoscale user interface for pooled VDI Delivery Groups:
Enable or disable Autoscale for a Delivery Group

**Note:**
By default, Autoscale is enabled when you create a Delivery Group.

1. On the Manage tab, select Delivery Groups in the Studio navigation pane.
2. In the Actions pane, select the Delivery Group you want to manage and then click Edit Delivery Group.
3. On the Autoscale page, select the Autoscale check box to enable Autoscale. After you enable Autoscale, the options on the page are enabled.
4. To disable Autoscale, clear the Autoscale check box. The options on the page turn gray to indicate that Autoscale is disabled for the selected Delivery Group.

**Important:**
- If you disable Autoscale, all machines managed by Autoscale will remain in the state they
are in at the time of disabling.

- After you disable Autoscale, the machines in drain state are taken out of drain state. For more information about drain state, see Drain state.

**How Autoscale power manages machines**

Autoscale powers machines on and off based on the selected schedule. Autoscale lets you set multiple schedules that include specific days of the week and adjust the number of machines available during those times. If you expect a set of users to consume the machine resources at a specific time on specific days, Autoscale helps provide an optimized experience. Note that those machines will be powered on during the schedule, irrespective of whether there are sessions running on them.

The schedule is based on the time zone of the Delivery Group. To change the time zone, you can change user settings in a Delivery Group. For more information, see Manage Delivery Groups.

Autoscale has two default schedules: **Weekdays** (Monday through Friday) and **Weekend** (Saturday and Sunday). By default, the **Weekdays** schedule keeps one machine powered on from 07:00 AM to 06:30 PM during peak times and none during off-peak times; the default capacity buffer is set to 10% during peak and off-peak times. By default, the **Weekend** schedule keeps no machines powered on.

**Note:**

Autoscale treats only those machines that are registered with the Site as part of the available capacity in the calculations it makes. “Registered” means that the machine is available for use or already in use. Doing so ensures that only machines that can accept user sessions are included in the capacity for the Delivery Group.

**Schedule-based settings**

**Autoscale schedule.** Lets you add, edit, select, and delete schedules.

**Days applied.** Highlights the days you applied to the selected schedule. The remaining days are grayed out.

**Edit.** Lets you assign the machines against each hour. You can assign the machines by numbers and by percentages.

**Note:**

- This option is available only in the Autoscale user interfaces for RDS and pooled VDI Delivery Groups.
- The histogram next to **Edit** plots the number or percentage of machines that are running in different time slots.
- You can assign machines against each time slot by clicking **Edit** above Peak times. Depend-
When you select the option from the dropdown in the **Machines to start** window, you can assign machines by numbers or by percentages.

- For RDS Delivery Groups, you can set the minimum number of running machines separately for each half-hour of the day. For pooled VDI Delivery Groups, you can set the minimum number of running machines separately for each hour of the day.

To define your own schedules, follow the steps below.

1. Select **Edit schedules** from the dropdown and then click **Add schedule**.

2. In the Edit Autoscale Schedules window, select the days you want to apply to each schedule. You can also delete schedules where applicable.

3. Click **Apply** to save the schedules and return to the Autoscale page.

4. Select the applicable schedule from the dropdown and set the applicable options for that schedule.

**Important:**

- Autoscale does not allow the same day to overlap in different schedules. For example, if you select Monday in schedule 2 after selecting Monday in schedule 1, Monday is automatically cleared in schedule 1.
- A schedule name is not case sensitive.
- A schedule name must not be blank or contain only spaces.
- Autoscale allows blank spaces between characters.
- A schedule name must not contain the following characters: \ / ; : * ? = < > | [ ] { } " ".
- Autoscale does not support duplicate schedule names. Enter a different name for each schedule.
- Autoscale does not support empty schedules. This means that schedules without days selected are not saved.

**Note:**

On the Autoscale page, the days included in the selected schedule are highlighted, while those not included are grayed out.

**Load-based settings**

**Peak times.** Lets you define the peak times for the days you applied in the selected schedule. You can do so by right-clicking the horizontal bar graph. After you define the peak times, the remaining, undefined times default to off-peak times. By **default**, the 7:00 AM to 7:00 PM time slot is defined as peak times for the days included in the selected schedule.
Important:
- For RDS Delivery Groups, the peak times bar graph is used for the capacity buffer.
- For VDI Delivery Groups, the peak times bar graph is used for the capacity buffer and controls the actions to be triggered after logoff and/or disconnection.

**Capacity buffer.** Lets you keep a buffer of powered-on machines. A lesser value decreases the cost. A greater value ensures an optimized user experience so that when launching sessions, users do not have to wait for additional machines to power on. By default, the capacity buffer is 10% for peak and off-peak times. If you set the capacity buffer to 0 (zero), users might have to wait for additional machines to power on when launching sessions. Autoscale lets you determine the capacity buffer separately for peak and off-peak times.

**Miscellaneous settings**

Tip:
- You can choose to configure the miscellaneous settings using the Broker PowerShell SDK. For more information, see [Broker PowerShell SDK commands](#).
- To understand the SDK commands associated with the when disconnected and when logged off settings, see [https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy](https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy).

**When disconnected.** Lets you specify how long a disconnected, locked machine remains powered on after session disconnection before it is suspended or shut down. If a time value is specified, the machine is suspended or shut down when the specified disconnection time is elapsed, depending on the actions you configured. By default, no action is assigned to disconnected machines. You can define options separately for peak and off-peak times. To do so, click the down arrow and then select one of the following options from the menu:

- **No action.** If selected, the machine after session disconnection remains powered on and Autoscale does not act on it.
- **Suspend.** If selected, Autoscale pauses the machine without shutting it down when the specified disconnection time is elapsed.
- **Shut down.** If selected, Autoscale shuts down the machine when the specified disconnection time is elapsed.

**Note:**
This option is available only in the Autoscale user interfaces for pooled and static VDI Delivery Groups.

**When logged off.** Lets you specify how long a machine remains powered on after session logoff before it is suspended or shut down. If a time value is specified, the machine is suspended or shut down when
the specified logoff time is elapsed, depending on the actions you configured. By default, no action is assigned to logged off machines. You can define options separately for peak and off-peak times. To do so, click the down arrow and then select one of the following options from the menu:

- **No action.** If selected, the machine after session logoff remains powered on and Autoscale does not act on it.
- **Suspend.** If selected, Autoscale pauses the machine without shutting it down when the specified logoff time is elapsed.
- **Shut down.** If selected, Autoscale shuts down the machine when the specified logoff time is elapsed.

**Note:**
This option is available only in the Autoscale user interface for static VDI Delivery Groups.

**Power-off delay.** Lets you specify the minimum number of minutes that must elapse after a machine is powered on before Autoscale powers it off. Doing so keeps machines from “flip-flopping” on and off during volatile session demands. By default, the power-off delay is 30 minutes. You can set it in a range of 0–60 minutes.

**Note:**
- For RDS Delivery Groups, this option is available only in the Autoscale user interface.
- For static VDI Delivery Groups, the power-off delay applies only to unassigned machines. To configure the power-off delay for static VDI Delivery Groups, use the PowerShell SDK. For example: `C:\PS> Set-BrokerDesktopGroup ”MyDesktop”-PowerOffDelay 15`.

**Machine instance cost per hour.** Lets you specify the machine instance cost per hour that matches with your cost basis. Machine instance cost per hour is the cost per hour, in US$, of the computing capacity being used. This setting is used to calculate the cost savings of the Autoscale settings above. To view the savings, go to Monitor > Trends > Machine Usage. For more information, see Monitor Autoscale-managed machines.

**Note:**
Autoscale does not support changing the currency unit for your cost basis.

**Power manage VDI machines transitioning to a different time period with disconnected sessions**

**Important:**
- This enhancement applies only to VDI machines with disconnected sessions. It does not apply to VDI machines with logged off sessions.
- For this enhancement to take effect, you need to enable Autoscale for the applicable Deliv-
Citrix Virtual Apps and Desktops service

ery Group. Otherwise, disconnect power policy actions are not triggered on period transition.

In earlier releases, a VDI machine transitioning to a time period where an action (disconnect action="Suspend" or "Shutdown") was required remained powered on. This scenario occurred if the machine disconnected during a time period (peak or off-peak times) where no action (disconnect action="Nothing") was required.

Starting with this release, Autoscale suspends or powers off the machine when the specified disconnection time elapses, depending on the disconnect action configured for the destination time period.

For example, you configure the following power policies for a VDI Delivery Group:

- Set PeakDisconnectAction to “Nothing”
- Set OffPeakDisconnectAction to “Shutdown”
- Set ‘OffPeakDisconnectTimeout’ to “10”

**Note:**


In earlier releases, a VDI machine with a session disconnected during peak times remained powered on when it transitioned from peak to off-peak. Starting with this release, the OffPeakDisconnectAction and the OffPeakDisconnectTimeout policy actions are applied to the VDI machine on period transition. As a result, the machine is powered off 10 minutes after it transitions to off-peak.

In case you want to revert to the previous behavior (that is, take no action on machines that transition from peak to off-peak or off-peak to peak with disconnected sessions), do one of the following:

- Set the “LegacyPeakTransitionDisconnectedBehaviour” registry value to 1 (true; enables the previous behavior). By default, the value is 0 (false; triggers disconnect power policy actions on period transition).
  - Path: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Name: LegacyPeakTransitionDisconnectedBehaviour
  - Type: REG_DWORD
  - Data: 0x00000001 (1)
- Configure the setting by using the Set-BrokerServiceConfigurationData PowerShell command. For example:
  - PS C:\> Set-BrokerServiceConfigurationData HostingManagement.
    LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true

A machine must meet the following criteria before power policy actions can be applied to it on period transition:
Citrix Virtual Apps and Desktops service

- Has a disconnected session.
- Has no pending power actions.
- Belongs to a VDI (single session) Delivery Group that transitions to a different time period.
- Has a session that disconnects during a certain time period (peak or off-peak times) and transitions to a period where a power action is assigned.

How capacity buffer works

Capacity buffer is used to add spare capacity to the current demand to account for dynamic load increases. There are two scenarios to be aware of:

- For RDS Delivery Groups, the capacity buffer is defined as a percentage of the total capacity of the Delivery Group in terms of load index. For more information about load index, see Load index.
- For VDI Delivery Groups, the capacity buffer is defined as a percentage of the total capacity of the Delivery Group in terms of the number of machines.

Autoscale lets you set the capacity buffer separately for peak and off-peak times. A lesser value in the capacity buffer field decreases the cost because Autoscale powers on less spare capacity. A greater value ensures an optimized user experience so that users do not have to wait for additional machines to power on when launching sessions. By default, the capacity buffer is 10%.

Important:

The capacity buffer results in machines being powered on when the total spare capacity drops to a level below “X” percent of the total capacity of the Delivery Group. Doing so reserves the required percentage of spare capacity.

RDS Delivery Groups

When are machines powered on?

Important:

If a schedule is selected, Autoscale powers on all machines configured to be powered on in the schedule. Autoscale keeps this specified number of machines powered on during the schedule, irrespective of the load.

When the number of powered-on machines in the Delivery Group can no longer meet the buffer needed for honoring the buffer capacity in terms of load index, Autoscale powers on extra machines. For example, let’s say your Delivery Group has 20 machines and 3 machines are scheduled to be powered on as part of schedule-based scaling with a capacity buffer of 20%; eventually 4 machines will be powered on when there is no load. This is because a 4 x 10k load index is needed as a buffer;
therefore at least 4 machines need to be powered on. This case might occur during peak times, increased load on machines, new session launches, and when you add new machines to the Delivery Group. Note that Autoscale powers on only the machines that meet the following criteria:

- The machines are not in maintenance mode.
- The hypervisor on which the machines are running is not in maintenance mode.
- The machines are currently powered off.
- The machines have no pending power actions.

**When are machines powered off?**

**Important:**

- If a schedule is selected, Autoscale powers off the machines based on the schedule.
- Autoscale does not power off the machines configured in the schedule to be powered on during the schedule.

When there are more than enough machines to support the targeted number of powered-on machines (including the buffer) for the Delivery Group, Autoscale powers off extra machines. This case might occur during off-peak times, decreased load on machines, and session logoffs, and when you remove machines from the Delivery Group. Autoscale powers off only the machines that meet the following criteria:

- The machines and the hypervisor on which the machines are running are not in maintenance mode.
- The machines are currently powered on.
- The machines are registered as available or waiting to register after start-up.
- The machines have no active sessions.
- The machines have no pending power actions.
- The machines satisfy the specified power-off delay. This means that the machines have been powered on for at least “X” minutes, where “X” is the power-off delay specified for the Delivery Group.

**Example scenario**

Suppose you have the following scenario:

- **Delivery Group configuration.** The Delivery Group that you want Autoscale to power manage contains 10 machines (M1 to M10).
- **Autoscale configuration**
Citrix Virtual Apps and Desktops service

- Capacity buffer is set to 10%.
- No machine is included in the selected schedule.

The scenario is executed in the following sequence:

1. No user logs on.
2. User sessions increase.
3. More user sessions start.
4. User session load decreases because of session termination.
5. User session load decreases further until the session load is handled only by on-premises resources.

See below for details about how Autoscale works in the scenario above.

- No user load (initial state)
  - One machine (for example, M1) is powered on. The machine is powered on because of the configured capacity buffer. In this case, 10 (number of machines) x 10,000 (load index) x 10% (configured capacity buffer) equals 10,000. Therefore, one machine is powered on.
  - The load index value of the powered-on machine (M1) is at a baseline load (load index equals 0).
- The first user logs on
  - The session is directed to be hosted on machine M1.
  - The load index of the powered-on machine M1 increases and machine M1 is no longer at a baseline load.
  - Autoscale starts to power on an additional machine (M2) to meet the demand because of the configured capacity buffer.
  - The load index value of machine M2 is at a baseline load.
- Users increase load
  - The sessions are load-balanced across machines M1 and M2. As a result, the load index of the powered-on machines (M1 and M2) increases.
  - The total spare capacity is still at a level above 10,000 in terms of load index.
  - The load index value of machine M2 is no longer at a baseline load.
- More user sessions start
  - The sessions are load-balanced across machines (M1 and M2). As a result, the load index of the powered-on machines (M1 and M2) increases further.
  - When the total spare capacity drops to a level below 10,000 in terms of load index, Autoscale starts to power on an additional machine (M3) to meet the demand because of the configured capacity buffer.
  - The load index value of machine M3 is at a baseline load.
- Even more user sessions start
The sessions are load-balanced across machines (M1 to M3). As a result, the load index of the powered-on machines (M1 to M3) increases.

The total spare capacity is at a level above 10,000 in terms of load index.

The load index value of machine M3 is no longer at a baseline load.

- **User session load decreases because of session termination**
  - After users log off their sessions or idle sessions time out, the freed-up capacity on machines M1 to M3 is reused to host sessions started by other users.
  - When the total spare capacity increases to a level above 10,000 in terms of load index, Autoscale puts one of the machines (for example, M3) into drain state. As a result, sessions started by other users are no longer directed to that machine unless new changes occur; for example, end-user load increases again or other machines become least loaded.

- **User session load continues to decrease**
  - After all sessions on machine M3 are terminated and the specified power-off delay times out, Autoscale powers off machine M3.
  - After more users terminate their sessions, the freed-up capacity on powered-on machines (M1 and M2) is reused to host sessions started by other users.
  - When the total spare capacity increases to a level above 10,000 in terms of load index, Autoscale puts one of the machines (for example, M2) into drain state. As a result, sessions started by other users are no longer directed to that machine.

- **User session load continues to decrease until there are no sessions**
  - After all sessions on machine M2 are terminated and the specified power-off delay times out, Autoscale powers off machine M2.
  - The load index value of the powered-on machine (M1) is at a baseline load. Autoscale does not put machine M1 into drain state because of the configured capacity buffer.

**Note:**

For RDS Delivery Groups, all changes to the desktop are lost when users log off sessions. However, if configured, user-specific settings are roamed along with the user profile.

**Pooled VDI Delivery Groups**

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the total number of machines in the Delivery Group. By default, the capacity buffer is 10% of the total number of machines in the Delivery Group.

If the number of machines (including the capacity buffer) exceeds the total number of currently powered-on machines, additional machines are powered on to meet the demand. If the number of machines (including the capacity buffer) is less than the total number of currently powered-on machines, the excess machines are shut down or suspended, depending on the actions you configured.
**Example scenario**

Suppose you have the following scenario:

- **Delivery Group configuration.** The Delivery Group that you want Autoscale to power manage contains 10 machines (M1 to M10).

- **Autoscale configuration**
  - Capacity buffer is set to 10%.
  - No machine is included in the selected schedule.

The scenario is executed in the following sequence:

1. No user logs on.
2. User sessions increase.
3. More user sessions start.
4. User session load decreases because of session termination.
5. User session load decreases further until the session load is handled only by on-premises resources.

See below for details about how Autoscale works in the scenario above.

- **No user load (initial state)**
  - One machine (M1) is powered on. The machine is powered on because of the configured capacity buffer. In this case, 10 (number of machines) x 10% (configured capacity buffer) equals 1. Therefore, one machine is powered on.

- **A first user logs on**
  - The first time a user logs on to use a desktop, the user is assigned a desktop from a pool of desktops hosted on powered-on machines. In this case, the user is assigned a desktop from machine M1.
  - Autoscale starts to power on an additional machine (M2) to meet the demand because of the configured capacity buffer.

- **A second user logs on**
  - The user is assigned a desktop from machine M2.
  - Autoscale starts to power on an additional machine (M3) to meet the demand because of the configured capacity buffer.

- **A third user logs on**
  - The user is assigned a desktop from machine M3.
  - Autoscale starts to power on an additional machine (M4) to meet the demand because of the configured capacity buffer.

- **A user logs off**
  - After a user logs off or the user’s desktop times out, the freed-up capacity (for example, M3) is available as buffer. As a result, Autoscale starts to power off machine M4 because
the capacity buffer is configured as 10%.

- More users log off until there are no users
  - After more users log off, Autoscale powers off machines (for example, M2 or M3).
  - Even though there are no users left, Autoscale does not power off the remaining one machine (for example, M1) because that machine is reserved as a spare capacity.

Note:
For pooled VDI Delivery Groups, all changes to the desktop are lost when users log off sessions. However, if configured, user-specific settings are roamed along with the user profile.

Static VDI Delivery Groups

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of unassigned machines powered on based on the total number of unassigned machines in the Delivery Group. By default, the capacity buffer is 10% of the total number of unassigned machines in the Delivery Group.

Important:
After all machines in the Delivery Group are assigned, the capacity buffer does not play a role in powering machines on or off.

If the number of machines (including the capacity buffer) exceeds the total number of currently powered-on machines, additional, unassigned machines are powered on to meet the demand. If the number of machines (including the capacity buffer) is less than the total number of currently powered-on machines, excess machines are powered off or suspended, depending on the actions you configured.

For Static VDI Delivery Groups, Autoscale:

- Powers assigned machines on during peak times and off during off-peak times only when the AutomaticPowerOnForAssigned property of the applicable VDI delivery group is set to true.
- Automatically powers on a machine during peak times if it is powered off and the AutomaticPowerOnForAssignedDuringPeak property of the Delivery Group to which it belongs is set to true.

To understand how capacity buffer works with assigned machines, consider the following:

- The capacity buffer works only when the Delivery Group has one or more unassigned machines.
- If the Delivery Group has no unassigned machines (all machines in the Delivery Group are assigned), the capacity buffer does not play a role in powering machines on or off.
- The AutomaticPowerOnForAssignedDuringPeak property determines whether assigned machines are powered on during peak times. If it is set to true, Autoscale keeps the machines powered on during peak times; Autoscale will also power them on even if they are powered off.
Example scenario

Suppose you have the following scenario:

- **Delivery Group configuration.** The Delivery Group that you want Autoscale to power manage contains 10 machines (M1 to M10).
- **Autoscale configuration**
  - Machines M1 to M3 are assigned, and machines M4 to M10 are unassigned.
  - Capacity buffer set to 10% for peak and off-peak times.
  - According to the selected schedule, Autoscale power manages machines between 09:00 AM and 06:00 PM.

See below for details about how Autoscale works in the scenario above.

- **Start of schedule – 09:00 AM**
  - Autoscale powers on machines M1 to M3.
  - Autoscale powers on an additional machine (for example, M4) because of the configured capacity buffer. Machine M4 is unassigned.
- **A first user logs on**
  - The first time a user logs on to use a desktop, the user is assigned a desktop from a pool of desktops hosted on unassigned powered-on machines. In this case, the user is assigned a desktop from machine M4. Subsequent logons from that user connect to the same desktop that was assigned on first use.
  - Autoscale starts to power on an additional machine (for example, M5) to meet the demand because of the configured capacity buffer.
- **A second user logs on**
  - The user is assigned a desktop from the unassigned powered-on machines. In this case, the user is assigned a desktop from machine M5. Subsequent logons from that user connect to the same desktop that was assigned on first use.
  - Autoscale starts to power on an additional machine (for example, M6) to meet the demand because of the configured capacity buffer.
- **Users log off**
  - As users log off their desktops or the desktops time out, Autoscale keeps the machines M1 to M5 powered on during 09:00 AM – 06:00 PM. When those users log on the next time, they connect to the same desktop that was assigned on first use.
  - The unassigned machine M6 is waiting to serve a desktop to an incoming, unassigned user.
- **End of schedule – 06:00 PM**
  - At 06:00 PM, Autoscale powers off machines M1 to M5.
  - Autoscale keeps the unassigned machine M6 powered on because of the configured capacity buffer. That machine is waiting to serve a desktop to an incoming, unassigned user.
  - In the Delivery Group, machines M6 to M10 are unassigned machines.
**Restrict Autoscale to certain machines in a Delivery Group**

Autoscale provides the flexibility to power manage only a subset of machines in a Delivery Group. To achieve this, apply a tag to one or more machines and then configure Autoscale to power manage only tagged machines.

This feature can be useful in cloud bursting use cases, where you want to use on-premises resources (or reserved public cloud instances) to handle workloads before cloud-based resources address additional demand (that is, burst workloads). To let on-premises machines (or reserved instances) address workloads first, you must use tag restriction along with zone preference.

Tag restriction specifies machines to be power managed by Autoscale. Zone preference specifies machines in the preferred zone to handle user launch requests. For more information, see [Tags](#) and [Zone preference](#).

**How to restrict Autoscale to machines in a Delivery Group**

There are two ways to restrict Autoscale to machines in a Delivery Group:

- Using the PowerShell SDK directly
- Using Studio along with the PowerShell SDK

To use the PowerShell SDK directly, complete the following steps:

1. **Create a tag.** Use the New-BrokerTag PowerShell command to create a tag.
   

2. **Apply the tag to machines.** Use the Get-BrokerMachine PowerShell command to apply the tag to machines in a catalog that you want Autoscale to power manage.
   
   • For example: `Get-BrokerMachine -CatalogName ”cloud” | Add-BrokerTag $managed.Name`. In this case, the catalog is named “cloud.”
   

**Note:**

You might add new machines to the catalog after applying the tag. The tag is NOT automatically applied to those new machines.
Add tagged machines to the Delivery Group that you want Autoscale to power manage.

Use the Get-BrokerDesktopGroup PowerShell command to add a tag restriction to the Delivery Group that contains the machines (in other words, “restrict launches to machines with tag X”).

- For example: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. In this case, the UID of the Delivery Group is 1.

To use Studio along with the PowerShell SDK, complete the following steps:

1. **Create a tag.** Use Studio to manually create a tag and to apply that tag to the applicable machines. For more information about how to use tags in Studio, see Tags.

2. **Fetch the tag.** Open PowerShell and then enter the Get-BrokerTag PowerShell command. For example: `$tag = Get-BrokerTag managed`. In this case, the tag you want Autoscale to restrict to is named “managed.”

3. **Add tagged machines to the Delivery Group that you want Autoscale to power manage.** In the PowerShell console window, enter the Get-BrokerDesktopGroup PowerShell command. For example: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $tag.Uid`. In this case, the UID of the Delivery Group is 1.

How to remove a tag restriction in a Delivery Group

After you apply the tag restriction, you might want to remove it from the Delivery Group later. To do so, use the Get-BrokerDesktopGroup PowerShell command.

Example: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $null`. In this case, the UID of the Delivery Group is 1.

Example scenario

Suppose you have the following scenario:

- **Machine catalog configuration.** There are two machine catalogs (C1 and C2).
  - Catalog C1 contains 5 machines (M1 to M5) that are local in the on-premises deployments.
  - Catalog C2 contains 5 machines (M6 to M10) that are remote in the cloud deployments.
- **Tag restriction.** A tag named “Cloud” is created and applied to machines M6 to M10 in catalog C2.
• **Zone configuration.** Two zones (Z1 and Z2) are created.
  - Zone Z1 containing catalog C1 corresponds to the on-premises deployments.
  - Zone Z2 containing catalog C2 corresponds to the cloud deployments.

• **Delivery Group configuration**
  - The Delivery Group contains 10 machines (M1 to M10), 5 machines from catalogs C1 (M1 to M5) and 5 from catalog C2 (M6 to M10).
  - Machines M1 to M5 are powered on manually and remain powered on throughout the schedule.

• **Autoscale configuration**
  - Capacity buffer is set to 10%.
  - Autoscale power manages only machines with the tag “Cloud.” In this case, Autoscale power manages cloud machines M6 to M10.

• **Published application or desktop configuration.** Zone preferences are configured for the published desktops (for example), where Zone Z1 is preferred over Zone Z2 for a user launch request.
  - Zone Z1 is configured as the preferred zone (home zone) for the published desktops.

The scenario is executed in the following sequence:

1. No user logs on.
2. User sessions increase.
3. User sessions increase further until all available on-premises machines are consumed.
4. More user sessions start.
5. User session decreases because of session termination.
6. User session decreases further until the session load is handled only by on-premises machines.

See below for details about how Autoscale works in the scenario above.

• **No user load (initial state)**
  - The on-premises machines M1 to M5 are all powered on.
  - One machine in the cloud (for example, M6) is powered on. The machine is powered on because of the configured capacity buffer. In this case, 10 (number of machines) x 10,000 (load index) x 10% (configured capacity buffer) equals 10,000. Therefore, one machine is powered on.
  - The load index value of all the powered-on machines (M1 to M6) is at a baseline load (load index equals 0).

• **Users log on**
  - The sessions are directed to be hosted on machines M1 to M5 through the configured zone preference and are load-balanced across these on-premises machines.
  - The load index value of the powered-on machines (M1 to M5) increases.
  - The load index value of the powered-on machine M6 is at a baseline load.
Citrix Virtual Apps and Desktops service

- Users increase load, consuming all on-premises resources
  - The sessions are directed to be hosted on machine M1 to M5 through the configured zone preference and are load-balanced across these on-premises machines.
  - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
  - The load index value of the powered-on machine M6 remains at a baseline load.
- One more user logs on
  - The session overflows the zone preference and is directed to be hosted on cloud machine M6.
  - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
  - The load index value of the powered-on machine M6 increases, but the total spare capacity is still at a level above 10,000 in terms of load index.
- More users log on
  - The sessions are directed to be hosted on machine M6.
  - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
  - The load index value of the powered-on machine M6 increases. When the total spare capacity drops to a level below 10,000 in terms of load index, Autoscale starts to power on an additional machine (M7) to meet the demand because of the configured capacity buffer. Note that it might take some time to power on machine M7. So there might be a delay until machine M7 is ready.
  - The load index value of the powered-on machine M7 remains at a baseline load.
- Even more users log on
  - After machine M7 is ready, the sessions are directed to be hosted on machines M6 and M7 and are load-balanced across these machines.
  - The load index value of all the powered-on machines (M1 to M5) has reached 10,000.
  - The load index value of machine M7 is no longer at a baseline load.
  - The load index value of the powered-on machines (M6 and M7) increases.
  - The total spare capacity is at a level above 10,000 in terms of load index.
- User session load decreases because of session termination
  - After users log off their sessions or idle sessions time out, the freed-up capacity on machines M1 to M7 is reused to host sessions started by other users.
  - When the total spare capacity increases to a level above 10,000 in terms of load index, Autoscale puts one of the cloud machines (M6 to M7) into drain state. As a result, sessions started by other users are no longer directed to that machine (for example, M7) unless new changes occur; for example, user load increases again or other cloud machines become least loaded.
- User session load decreases further until one or more cloud machines are no longer needed
  - After all sessions on machine M7 are terminated and the specified power-off delay times out, Autoscale powers off machine M7.
  - The load index value of all the powered-on machines (M1 to M5) might drop to a level below
10,000.
- The load index value of the powered-on machine (M6) decreases.
- User session decreases further until no cloud machines are needed.
- Even though there are no user sessions on machine M6, Autoscale does not power it off because it is reserved as a spare capacity.
- Autoscale keeps the remaining cloud machine M6 powered on because of the configured capacity buffer. That machine is waiting to serve a desktop to an incoming user.
- Sessions are not directed to be hosted on machine M6 as long as the on-premises machines have available capacity.

**Monitoring metrics**

You can monitor the following metrics of Autoscale-managed machines from the Monitor tab.

- Machine usage
- Estimated savings
- Alert notifications for machines and sessions
- Machine status
- Load evaluation trends

For more information about the metrics, see Monitor Autoscale-managed machines.

**Broker PowerShell SDK commands**

You can configure Autoscale for Delivery Groups using the Broker PowerShell SDK. To configure Autoscale using PowerShell commands, you must use Remote PowerShell SDK version 7.21.0.12 or later. For more information about the Remote PowerShell SDK, see SDKs and APIs.

**Set-BrokerDesktopGroup**

Disables or enables an existing BrokerDesktopGroup or alters its settings. For more information about this cmdlet, see [https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/](https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/).

**New-BrokerPowerTimeScheme**

Examples

See the following examples for details about how to use the PowerShell cmdlets.

Enable Autoscale

• Suppose you want to enable Autoscale for the Delivery Group whose name is “MyDesktop.” Use
the Set-BrokerDesktopGroup PowerShell command. For example:
  – PS C:\> Set-BrokerDesktopGroup ”MyDesktop”-AutoscalingEnabled $true

Configure the capacity buffer separately for peak and off-peak times

• Suppose you want to set the capacity buffer to 20% for peak times and 10% for off-peak times
for a Delivery Group whose name is “MyDesktop.” Use the Set-BrokerDesktopGroup PowerShell
command. For example:
  – PS C:\> Set-BrokerDesktopGroup ”MyDesktop”-PeakBufferSizePercent 20
  – OffPeakBufferSizePercent 10

Configure the when disconnected timeout

• Suppose you want to set the when disconnected timeout to 60 minutes for peak times and
30 minutes for off-peak times for a Delivery Group whose name is “MyDesktop.” Use the Set-
BrokerDesktopGroup PowerShell command. For example:
  – PS C:\> Set-BrokerDesktopGroup ”MyDesktop”-PeakDisconnectTimeout 60
  – OffPeakDisconnectTimeout 30

Configure the when logged off timeout

• Suppose you want to set the when logged off timeout to 60 minutes for peak times and
30 minutes for off-peak times for a Delivery Group whose name is “MyDesktop.” Use the
Set-BrokerDesktopGroup PowerShell command. For example:
  – PS C:\> Set-BrokerDesktopGroup ”MyDesktop”-PeakLogOffTimeout 60
  – OffPeakLogOffTimeout 30

Configure the power-off delay

• Suppose you want to set the power-off delay to 15 minutes for a Delivery Group whose name is
“MyDesktop.” Use the Set-BrokerDesktopGroup PowerShell command. For example:
  – PS C:\> Set-BrokerDesktopGroup ”MyDesktop”-PowerOffDelay 15

Configure the machine instance cost

• Suppose you want to set the machine instance cost per hour to 0.2 dollars for a Delivery Group
whose name is “MyDesktop.” Use the Set-BrokerDesktopGroup PowerShell command. For ex-
ample:
  – PS C:\> Set-BrokerDesktopGroup ”MyDesktop”-MachineCost 0.2

Create a power time scheme
Suppose you want to create a new power time scheme for a Delivery Group whose UID value is 3. The new scheme covers weekend, Monday, and Tuesday. The 8:00 AM to 6:30 PM time slot is defined as peak times for the days included in the scheme. For peak times, the pool size (the number of machines kept powered on) is 20. For off-peak times, it is 5. You can use the `Set-BrokerDesktopGroup PowerShell` command. For example:

```powershell
PS C:\> $ps48 = (0..47 | %{ if ($_.lt 16 -or $_.gt 37){ 5 } else { 20 } })
PS C:\> $pt48 = (0..47 | %{ if ($_.lt 16 -or $_.gt 37){ $false } else { $true } })
PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48
```

### Autoscale API

The Autoscale API provides a set of REST APIs that you can use to configure Autoscale. For more information about the complete set of available APIs for Autoscale, see [Citrix Cloud APIs](#).

### Good to know

Autoscale works at a Delivery Group level. It is configured on a per-Delivery Group basis. It power manages only the machines in the selected Delivery Group.

### Drain state

Autoscale always attempts to scale down the number of powered-on machines in the Delivery Group to the configured pool size and capacity buffer. It does so by putting the excess machines with the fewest sessions into “drain state” and powering them off when all sessions are logged off. This occurs when session demand lessens and the schedule requires fewer machines than are powered on.

Autoscale puts excess machines into “drain state” one by one. If two or more machines have the same number of active sessions, Autoscale drains the machine that has been powered on for the specified power-off delay. Doing so avoids putting recently powered-on machines into drain state because those machines are more likely to have the fewest sessions. If two or more machines have been powered on for the specified power-off delay, Autoscale drains those machines one by one at random.

Machines in drain state no longer host new session launches and are waiting for the existing sessions to be logged off. A machine becomes a candidate for shutdown only when all sessions are logged off. However, if there are no machines immediately available for session launches, Autoscale prefers directing the session launches to a machine in drain state over powering on a machine.
A machine is taken out of drain state when one of the following conditions is met:

- The machine is powered off.
- Autoscale is disabled for the Delivery Group to which the machine belongs.
- Autoscale utilizes the machine to meet schedule or load demand requirements. This case occurs when the schedule (schedule-based scaling) or the current demand (load-based scaling) requires more machines than are currently powered on.

**Important:**

If no machines are immediately available for session launches, Autoscale prefers directing session launches to a machine in drain state over powering on a machine. A machine in drain state that hosts a session launch remains in drain state.

To find out which machines are in drain state, use the Get-BrokerMachine PowerShell command. For example: `Get-BrokerMachine -DrainingUntilShutdown $true`.

**Load index**

**Important:**

Load index does not apply to VDI Delivery Groups. It applies only to RDS Delivery Groups.

The load index value ranges from 0 to 10,000, which is calculated using the Citrix Load Management policy settings configured for concurrent logon, session, CPU, disk, and memory use. The digit “0” indicates a completely unloaded machine. A machine with a load index value of 0 is at a baseline load. The digit “10,000” indicates a fully loaded machine that cannot run any more sessions. The load index metric determines how likely a machine is to receive connections. By default, a machine is considered at full load when it is hosting 250 sessions.

**Capacity and machine registration**

To ensure that Autoscale has an accurate view of machines that can accept session requests, Autoscale includes only machines that are registered with the Site when determining the capacity for a given Delivery Group. Powered-on machines that are unregistered cannot accept session requests. As a result, they are not included in the overall capacity of the Delivery Group.

**Scaling across multiple Machine Catalogs**

In some Sites, multiple machine catalogs might be associated with a single Delivery Group. Autoscale randomly powers on machines from each catalog to meet schedule or session demand requirements.
For example, a Delivery Group has two machine catalogs: Catalog A has three machines powered on and Catalog B has one machine powered on. If Autoscale needs to power on an additional machine, it might power on a machine from either Catalog A or Catalog B.

**Machine provisioning and session demand**

The Machine Catalog associated with the Delivery Group must have enough machines to power on and off as demand increases and decreases. If session demand exceeds the total number of registered machines in the Delivery Group, Autoscale only ensures that all registered machines are powered on. **Autoscale does not provision additional machines.**

**Availability of monitoring data**

Monitoring data is available when Autoscale is enabled for the Delivery Group. Monitoring data continues to be available when Autoscale is enabled and then disabled for the Delivery Group. Autoscale collects monitoring data at 5-minute intervals.

**Note:**

When you initially enable Autoscale for a Delivery Group, it might take a few minutes to display monitoring data for that Delivery Group.

**Instance size considerations**

You can optimize your costs if you right size your instances in public clouds. Smaller instances host fewer user sessions than larger instances. Therefore, in the case of smaller instances, Autoscale puts machines into drain state much faster because it takes less time for the last user session to be logged off. As a result, Autoscale powers off smaller instances sooner, thereby reducing costs. Citrix recommends that you provision smaller instances as long as they match your workload performance and capacity requirements.

**Configuration Logging**

July 30, 2019

Configuration Logging captures Citrix Virtual Apps and Desktops deployment configuration changes and administrative activities to a logging database in Citrix Cloud. You can use the logged content to:

- Diagnose and troubleshoot problems after configuration changes are made. The log provides a breadcrumb trail.
Citrix Virtual Apps and Desktops service

- Assist change management and track configurations.
- Report administration activity.

From Studio, you can view configuration log content, filtered by date ranges or by full text search. You can also generate a CSV report using PowerShell. From Studio, you cannot edit or delete log content. You can use the Remote PowerShell SDK to schedule periodic data deletion from the log.

Configuration logs are localized when they are created. For example, a log created in English is read in English, regardless of the locale of the reader.

Permissions required (see Delegated Administration):
- Full Administrators in Citrix Cloud, plus Citrix Virtual Apps and Desktops service Cloud Administrators and Read Only Administrators can view configuration logs in Studio.
- Full Administrators and Cloud Administrators can also download a CSV report of logging activity, using PowerShell.

What is logged

Configuration changes and administrative activities initiated from the service’s Studio (Manage), Director (Monitor), and PowerShell scripts are logged. However, you cannot see log entries for Citrix Cloud platform internal operations, such as database setup and management.

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
- Manage or monitor functions sending a message to a user

The following operations are not logged. (Many are not available to customer administrators.)
- 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 or from sources other than Studio (Manage), Director (Monitor), or PowerShell.
Display configuration log content

1. Sign in to Citrix Cloud. Select Virtual Apps and Desktops in the upper left menu.
2. Select the Manage tab.
3. 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. You can:

- Sort the display by column heading.
- Filter the display by specifying a day interval, or entering text in the Search box. To return to the standard display after using search, clear the text in the Search box.

Display characteristics:

- High-level operations created during management and monitoring are listed in the upper middle pane in Studio. A high-level operation results in one or more services and PowerShell SDK calls, which are low-level operations. When you select a high-level operation in the upper middle pane, the lower pane displays the low-level operations.
- If you create a low-level operation in PowerShell without specifying a parent high-level operation, Configuration Logging creates a surrogate high-level operation.
- 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 logs for the last five days are requested, and a log with a start time in the last five days has no end time, it is included.
- Remember: You cannot see log entries for Citrix Cloud platform internal operations, such as database setup and management.

Generate reports

To generate a report containing configuration log data, use PowerShell cmdlets for the ConfigLogging Service in the Citrix Virtual Apps and Desktops Remote PowerShell SDK. For example, you can retrieve a filtered list of high-level or low-level operations. For details, see SDKs and APIs and Citrix Virtual Apps and Desktops SDK.

Schedule periodic data deletion

Use the Remote PowerShell SDK to specify how long data is retained in the Configuration Logging database. (This feature is not available in the Studio management console.) In the Citrix Virtual Apps and Desktops service, you must have Full access.
In the `Set-LogSite` cmdlet, the `-LoggingDBPurgeDurationDays` parameter specifies how many days data in the Configuration Logging database is retained before it is deleted automatically.

- By default, the value of this parameter is 0. A zero value means that data in the Configuration Logging database is never deleted automatically.
- When you set a non-zero value, the database is checked once every 120 minutes. Data older than the retention period is deleted.

Use `Get-LogSite` to view the current value of the parameter.

**Differences from on-premises Citrix Virtual Apps and Desktops**

If you're familiar with Configuration Logging in the on-premises Virtual Apps and Desktops product, the Citrix Cloud version has several differences.

In Citrix Cloud:

- Configuration Logging is always enabled. You cannot disable it. Mandatory logging is not available.
- You cannot change the location of the Configuration Logging database, because the database is managed in the Citrix Cloud platform, and is accessible by customer administrators.
- Configuration log displays do not include operations and activities that are performed within the Citrix Cloud platform.
- You can create a CSV report of logged operations using PowerShell cmdlets only. In the on-premises product, CSV or HTML reports can be generated from Studio or PowerShell.
- You cannot delete configuration log content.

**Delegated Administration**

June 27, 2019

**Overview**

With Delegated Administration in Citrix Cloud, you can configure the access permissions that all of your administrators need, in accordance with their role in your organization.

By default, administrators have full access. This setting enables access to all available customer administration and management functions in Citrix Cloud, plus all subscribed services. To tailor an administrator’s access:

- Configure custom access for an administrator’s general management permissions in Citrix Cloud.
- Configure custom access for subscribed services. In the Citrix Virtual Apps and Desktops service, you can configure custom access when you invite a new administrator. You can change an administrator’s access later.

Details about displaying the list of administrators and defining access permissions are available in Add administrators to a Citrix Cloud account.

This article describes how to configure custom access in the Citrix Virtual Apps and Desktops service.

Administrators, roles, and scopes

Delegated Administration uses three concepts for custom access: administrators, roles, and scopes.

- **Administrators**: An administrator represents a person identified by their Citrix Cloud sign-in, which is typically an email address. Each administrator is associated with one or more role and scope pairs.

- **Roles**: A role represents a job function, and has permissions associated with it. These permissions allow certain tasks that are unique to the service. For example, the Delivery Group Administrator role has permission to create a Delivery Group and remove a desktop from a Delivery Group, plus other associated permissions. An administrator can have multiple roles. An administrator might be a Delivery Group Administrator and a Machine Catalog Administrator.

The service offers several built-in custom access roles. You cannot change the permissions within these built-in roles, or delete those roles.

You can create your own custom access roles to meet your organization’s requirements, and delegate permissions with more detail. Use custom roles to allocate permissions at the granularity of an action or task. You can delete a customized role only if it is not assigned to an administrator.

You can change which roles an administrator has.

A role is always paired with a scope.

- **Scopes**: A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to your organization. Objects can be in more than one scope.

There is one built-in scope: All, which contains all objects. Citrix Cloud and Help Desk administrators are always paired with the All scope. That scope cannot be changed for those administrators.

When you invite (add) an administrator for this service, a role is always paired with a scope (by default, the All scope).

You create and delete scopes in the service’s Manage console. You assign role/scope pairs in the Citrix Cloud console.
A scope is not shown for Full access administrators. By definition, those administrators have access to all customer-managed Citrix Cloud and subscribed services objects.

**Built-in roles and scopes**

The service has the following built-in roles.

- **Cloud Administrator:** Can perform all tasks that can be initiated from the service.
  
  Can see the Manage and Monitor tabs in the console. This role is always combined with the All scope, you cannot change the scope.
  
  Do not be confused by this role’s name. A custom access Cloud Administrator cannot perform Citrix Cloud-level tasks (Citrix Cloud tasks require Full access).

- **Read Only Administrator:** Can see all objects in the specified scopes (in addition to global information), but cannot change anything. For example, a Read Only Administrator with Scope=London can see all global objects 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).
  
  Can see the Manage tab in the console, cannot see the Monitor tab. You can change the scope.

- **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. Can also perform session management and machine power management operations for the machines in those Delivery Groups.
  
  Can see the Monitor tab in the console, cannot see the Manage tab. This role is always combined with the All scope, you cannot change the scope.

- **Machine Catalog Administrator:** Can create and manage machine catalogs and provision the machines into them. Can manage base images and install software, but cannot assign applications or desktops to users.
  
  Can see the Manage tab in the console, cannot see the Monitor tab. You can change the scope.

- **Delivery Group Administrator:** Can deliver applications, desktops, and machines. Can also manage the associated sessions. Can manage application and desktop configurations such as policies and power management settings.
  
  Can see the Manage tab in the console, cannot see the Monitor tab. You can change the scope.

- **Host Administrator:** Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to users.
  
  Can see the Manage tab in the console, cannot see the Monitor tab. You can change the scope.
The following table summarizes which console tabs are visible for each custom access role in the service, and whether the role can be used with custom scopes.

<table>
<thead>
<tr>
<th>Custom access administrator role</th>
<th>Can see <strong>Manage</strong> tab in console?</th>
<th>Can see <strong>Monitor</strong> tab in console?</th>
<th>Can role be used with custom scopes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Administrator</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Read Only Administrator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Help Desk Administrator</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Machine Catalog Administrator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Delivery Group Administrator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Host Administrator</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To view the permissions associated with a role:

1. Sign in to **Citrix Cloud** if you haven’t already. Select **My Services > Virtual Apps and Desktops** in the upper left menu. Select the **Manage** tab.

2. Click **Configuration > Administrators** in the navigation pane and then click the **Roles** tab.

3. Select a role in the upper middle pane. The **Role definition** tab in the lower pane lists the categories and permissions. Select a category to see the specific permissions. The **Administrators** tab lists the administrators who have been assigned the selected role.

   Known issue: A Full Administrator entry in the **Manage** console does not display the correct set of permissions for a full access service administrator.

**How many administrators you need**

The number of administrators and the granularity of their permissions generally depend 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 custom access delegation. In this case, each administrator has Full access, which always 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).
example, two have Full access, and others are Help Desk Administrators. Also, an administrator
might manage only certain groups of objects (scopes), such as machine catalogs in a particular
department. In this case, create new scopes, plus administrators with the appropriate custom
access role and scopes.

Administrator management summary

Setting up administrators for the service follows this sequence:

1. If you want the new administrator to have a role other than a Full administrator (which covers
   all subscribed services in Citrix Cloud) or a built-in role, create a custom role.
2. If you want the new administrator to have a scope other than All (and a different scope is allowed
   for the intended role, and has not already been created), create scopes.
3. From Citrix Cloud, invite an administrator. If you want the new administrator to have anything
   other than the default Full access, specify a custom access role and scope pair.

Later, if you want to change an administrator’s access (roles and scope), see Configure custom access.

Invite an administrator

Adding administrators follows the guidance detailed in Add administrators to a Citrix Cloud account.
A subset of that information is repeated here.

Important:

Do not confuse how “custom” and “custom access” are used.

- When creating administrators and assigning roles for the service in the Citrix Cloud console,
  the term “custom access” includes both the built-in roles and any additional custom roles
  that were created in the service’s Manage console.
- In the service's Manage console, “custom” simply differentiates that role from a built-in
  role.

To add and invite an administrator:

1. After signing into Citrix Cloud, select Identity and Access Management in the upper left menu.
2. On the Identity and Access Management page, click Administrators. The display lists the cur-
   rent administrators in the account.
3. Click Add administrators from, and then select your authentication method. Enter the per-
   son’s email address. Optionally, select a role and scope pair.

   If you do not select a custom access role and scope pair, the new administrator is assigned full
   access by default. That setting includes access to all customer administrator functions in Citrix
   Cloud and in all subscribed services.
If you want that administrator to have more limited access, select a custom access role and scope pair. In that way, new administrators have the intended permissions when they sign in to Citrix Cloud for the first time.

4. Click **Invite**. Citrix Cloud sends an invitation to the email address you specified and adds the administrator to the list.

When the administrator receives the email, they click the **Join** link to accept the invitation.

**Create and manage roles**

When administrators create or edit a role, they can enable only the permissions that they themselves have. This prevents administrators from creating a role with more permissions than they currently have and then assigning it to themselves (or editing a role that they are already assigned).

Custom role names can contain up to 64 Unicode characters. They cannot contain: 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.

Role descriptions can contain up to 256 Unicode characters.

1. Sign in to **Citrix Cloud** if you haven’t already. Select **My Services > Virtual Apps and Desktops** in the upper left menu. Select the **Manage** tab.

2. Click **Configuration > Administrators** in the navigation pane, and then click the **Roles** tab in the upper middle pane.

3. Follow the instructions for the task you want to complete:

   - **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.

   - **Create a custom role**: Click **Create new Role** in the Actions pane. Enter a name and description. Select the object types and permissions. When you’re done, click **Save**.
• **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. When you’re done, click **Save**.

• **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. You cannot edit a built-in role. When you’re done, click **Save**.

• **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. You cannot delete a built-in role. You cannot delete a custom role if it is assigned to an administrator.

**Create and manage scopes**

By default, all roles have the All scope for their relevant objects. For example, a Delivery Group Administrator can manage all Delivery Groups. For some administrator roles, you can create a scope that allows that administrator role to access a subset of the relevant objects. For example, you might want a give a Machine Catalog Administrator access to only catalogs that contain a certain type of machines, rather than all catalogs.

• Full access administrators or custom access Cloud Administrators can create scopes for the Read Only Administrator, Machine Catalog Administrator, Delivery Group Administrator, and Host Administrator roles.
Citrix Virtual Apps and Desktops service

- Scopes cannot be created for Full access administrators, nor can they be created for Cloud Administrators or Help Desk Administrators, because those administrators always have the All scope.

Rules for creating and managing scopes:

- Scope names can contain up to 64 Unicode characters. Scope names cannot include: backslash, forward slash, semicolon, colon, pound sign, comma, asterisk, question mark, equal sign, left or right arrow, pipe, left or right bracket, left or right parenthesis, quotation marks, and apostrophe.
- Scope 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 an administrator. If the edited scope is paired with one or more roles, ensure that your scope updates do not make any role/scope pair unusable.

To create and manage scopes:

1. Sign in to Citrix Cloud if you haven’t already. Select My Services > Virtual Apps and Desktops in the upper left menu. Select the Manage tab.
2. Click Configuration > Administrators in the navigation pane and then click the Scopes tab in upper middle pane.
3. Follow the instructions for the task you want to complete:
   - **View scope 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.
   - **Create a scope**: Click Create Scope in the Actions pane. Enter a name and description. The objects are listed by type, such as Delivery Group and Machine Catalog.
     - To include all objects of a particular type (for example, all Delivery Groups), select the check box for the object type.
     - To include individual objects within a type, expand the type and then select the check boxes for the objects (for example, specific Delivery Groups).

When you’re done, click Save.
• **Copy a scope:** Select the scope in the middle pane and then click **Copy Scope** in the Actions pane. Change the name, description. Change the object types and objects, as needed. When you’re done, click **Save**.

• **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. When you’re done, click **Save**.

• **Delete a scope:** Select the scope in the middle pane and then click **Delete Scope** in the Actions pane. When prompted, confirm the deletion.

  You cannot delete a scope if it is assigned to a role. If you attempt to do this, an error message indicates that you do not have permission. In fact, the error occurs because the role/scope pair that uses this scope is assigned to an administrator. First, remove the role/scope pair assignment for all administrators who use it. Then delete the scope in the **Manage** console.

After you create a scope, it appears in the **Custom access** list in the Citrix Cloud console, paired with its appropriate role. You can then assign it to an administrator.

For example, let’s say you create a scope named CAD, and select the machine catalogs that contain machines suitable for CAD applications. When you return to the Citrix Cloud console, the list of service-
level custom access role/scope pairs now has new entries (shown in bold):

- Cloud Administrator, All
- Delivery Group Administrator, All
- Delivery Group Administrator, CAD
- Help Desk Administrator, All
- Host Administrator, All
- Host Administrator, CAD
- Machine Catalog Administrator, CAD
- Machine Catalog Administrator, All
- Machine Catalog Administrator, CAD
- Read Only, All
- Read Only, CAD

The Cloud Administrator and Help Desk Administrator always have the All scope, so the CAD scope does not apply to them.

**Configure custom access for an administrator**

By default, when you invite administrators, they have Full access.

Remember: Full access allows the administrator to manage all subscribed services plus customer administrator Citrix Cloud operations (such as inviting more administrators). A Citrix Cloud deployment needs at least one administrator with Full access.

To configure custom access for an administrator:

1. Sign in to Citrix Cloud if you haven’t already. Select **Identity and Access Management > Administrators** in the upper left menu.
2. Locate the administrator you want to manage, click the ellipsis menu, and select **Edit access**.
3. Select **Custom access**. To configure service-specific custom access, under **Virtual Apps and Desktops**, select or clear the check marks next to one or more role and scope pairs in the Custom access list.

   If you have not created any scopes and assigned them to a role, every role in the Custom access list has the All scope. For example, the role/scope entry **Delivery Group Administrator, All** indicates that role has the All scope.

   When you create a role or scope, it appears in the custom access list for the service and can be selected. For example, if you created a scope named Catalog1, the Custom access list includes a **Machine Catalog Administrator, Catalog1** entry, in addition to the default **Machine Catalog Administrator, All** entry.

4. If the administrator you’re editing already has custom access and you want to give that administrator full access, select **Full access**.
5. When you’re done, click **Save**.

The following screenshot shows the full access and the custom access built-in administrator roles.
Citrix Virtual Apps and Desktops service

Custom Access requires at least one role to be selected.

- **Full access**
  Full access allows administrators management control of Citrix Cloud and its services, as well as the ability to create and manage virtual desktops and applications.

- **Custom access**
  Switching to custom access will remove management access to certain services. Custom access allows you to determine exactly which part of Citrix Cloud your administrators can access.

  Select all

  - General Management
    - Domains
    - Library
    - Notifications
    - Resource Location

  - Virtual Apps and Desktops
    - Cloud Administrator, All
    - Delivery Group Administrator, All
    - Help Desk Administrator, All - Access to 'Monitor' tab only
    - Host Administrator, All
    - Machine Catalog Administrator, All
    - Read Only Administrator, All
Differences from on-premises Citrix Virtual Apps and Desktops

If you’re familiar with Delegated Administration in the on-premises Citrix Virtual Apps and Desktops version, the service version has several differences.

In Citrix Cloud:

- Administrators are identified by their Citrix Cloud login, rather than their Active Directory account. You can create role/scope pairs for Active Directory individuals, but not groups.
- Administrators are created, configured, and deleted in the Citrix Cloud console, rather than the service’s Manage console (Studio).
- Role/scope pairs are assigned to administrators in the Citrix Cloud console, rather than the service’s Manage console (Studio).
- Reports are not available. You can view administrator, role, and scope information in the Manage console.
- The custom access Cloud Administrator is similar to a Full Administrator in the on-premises version. Both have full management and monitoring permissions for the Citrix Virtual Apps and Desktops version being used. However, in the service, there is no named Full Administrator role. Do not equate “Full access” in Citrix Cloud with the “Full administrator” in on-premises Citrix Virtual Apps and Desktops. Full access in Citrix Cloud spans the platform-level domains, library, notifications, and resource locations, plus all subscribed services.

Differences from earlier service releases

Before the release of the expanded custom access feature (September 2018), there were two custom access administrator roles: Full Administrator and Help Desk Administrator. When your deployment has Delegated Administration enabled (which is a platform setting), those roles are mapped automatically.

- An administrator who was formerly configured as a custom access Virtual Apps and Desktops (or XenApp and XenDesktop) Service: Full Administrator is now a custom access Cloud Administrator.
- An administrator who was formerly configured as a custom access Virtual Apps and Desktops (or XenApp and XenDesktop) Service: Help Desk Administrator is now a custom access Help Desk Administrator.

More information

See Delegated Administration and Monitoring for information about administrators, roles, and scopes used in the service’s Monitor console.
Local Host Cache

August 28, 2019

The Local Host Cache (LHC) feature enables connection brokering operations in a Citrix Virtual Apps and Desktops service deployment to continue when a Cloud Connector cannot communicate with Citrix Cloud. Local Host Cache engages when the network connection is lost for 20 seconds.

With Local Host Cache, users who are connected when an outage occurs can continue working uninterrupted. Reconnections and new connections experience minimal connection delays.

Important:
Each satellite zone (resource location) must have an on-premises StoreFront installed and configured. Local Host Cache works only in resource locations containing an on-premises StoreFront.

Data content

Local Host Cache includes the following information, which is a subset of the information in the main database:

- Identities of users and groups who are specifically assigned rights to resources published from the Site.
- Identities of users who are currently using, or who have recently used, published resources from the Site.
- Identities of VDA machines (including Remote PC Access machines) configured in the Site.
- Identities (names and IP addresses) of client Citrix Workspace app machines being actively used to connect to published resources.

It also contains information for currently active connections that were established while the main database was unavailable:

- Results of any client machine endpoint analysis performed by Citrix Workspace app.
- Identities of infrastructure machines (such as Citrix Gateway and StoreFront servers) involved with the Site.
- Dates and times and types of recent activity by users.

How it works

During normal operations:
• The Brokering Principal (Citrix Remote Broker Provider Service) on a Cloud Connector accepts connection requests from StoreFront, and communicates with Citrix Cloud to connect users with VDAs that are registered with the Cloud Connector.

• The Citrix Config Synchronizer Service (CSS) checks with the broker in Citrix Cloud approximately every two minutes to see if any configuration changes have been made. Those changes can be administrator-initiated (such as changing a Delivery Group property) or system actions (such as machine assignments).

• If a configuration change has occurred since the previous check, the CSS synchronizes (copies) information to a secondary broker (Citrix High Availability Service, HA broker in the figure above) on the Cloud Connector. All configuration data is copied, not just items that have changed since the previous check. The secondary broker imports the data into a Microsoft SQL Server Express LocalDB database on the Cloud Connector. The CSS ensures that the information in the secondary broker’s LocalDB database matches the information in the site database in Citrix Cloud. The LocalDB database is re-created each time synchronization occurs.

The LocalDB database is installed automatically when you install a Cloud Connector. That database cannot be shared across Cloud Connectors. You do not need to back up this database; it is recreated every time a configuration change is detected.

• If no changes occurred since the last check, the configuration data is not copied.

During an outage:
When an outage begins:

- The secondary broker starts listening for and processing connection requests.
- When the outage begins, the secondary broker does not have current VDA registration data, but as soon as a VDA communicates with it, a registration process is triggered. During that process, the secondary broker also gets current session information about that VDA.
- While the secondary broker is handling connections, the Brokering Principal continues to monitor the connection to Citrix Cloud. When the connection is restored, the Brokering Principal instructs the secondary broker to stop listening for connection information, and the Brokering Principal resumes brokering operations. The next time a VDA communicates with the Brokering Principal, a registration process is triggered. The secondary broker removes any remaining VDA registrations from the previous outage. The CSS resumes synchronizing information when it learns that configuration changes have occurred in Citrix Cloud.

In the unlikely event that an outage begins during a synchronization, the current import is discarded and the last known configuration is used.

The event log indicates when synchronizations and outages occur.

There is no time limit imposed for operating in outage mode.

You can also intentionally trigger an outage. See Force an outage for details about why and how to do this.
Resource locations (satellite zones) with multiple Cloud Connectors

Among its other tasks, the CSS routinely provides the secondary broker with information about all Cloud Connectors in the resource location. Having that information, each secondary broker knows about all peer secondary brokers.

The secondary brokers communicate with each other on a separate channel. They use an alphabetical list of FQDN names of the machines they’re running on to determine (elect) which secondary broker will be in charge of brokering operations in the zone if an outage occurs. During the outage, all VDAs re-register with the elected secondary broker. The non-elected secondary brokers in the zone will actively reject incoming connection and VDA registration requests.

If an elected secondary broker fails during an outage, another secondary broker is elected to take over, and VDAs register with the newly elected secondary broker.

During an outage, if a Cloud Connector is restarted:

- If that Cloud Connector is not the elected primary broker, the restart has no impact.
- If that Cloud Connector is the elected primary broker, a different Cloud Connector is elected, causing VDAs to register. After the restarted Cloud Connector powers on, it automatically takes over brokering, which causes VDAs to register again. In this scenario, performance can be affected during the registrations.

The event log provides information about elections.

Design considerations and requirements

There is no time limit imposed for operating in outage mode. However, if the outage is due to local loss of Citrix Cloud connectivity from their resource location, customers should restore connectivity from their affected resource location as quickly as possible.

What is unavailable during an outage, and other differences

- You cannot use Studio or run PowerShell cmdlets.
- Monitoring data is not sent to Citrix Cloud during an outage. So, the Monitor functions (Director) do not show activity from an outage interval.
- Hypervisor credentials cannot be obtained from the Host Service. All machines are in the unknown power state, and no power operations can be issued. However, VMs on the host that are powered-on can be used for connection requests.
- An assigned machine can be used only if the assignment occurred during normal operations. New assignments cannot be made during an outage.
- Automatic enrollment and configuration of Remote PC Access machines is not possible. However, machines that were enrolled and configured during normal operation are usable.
Citrix Virtual Apps and Desktops service

- Server-hosted applications and desktop users may use more sessions than their configured session limits, if the resources are in different zones.
- Users can launch applications and desktops only from registered VDAs in the zone containing the currently active/elected High Availability Service. Launches across zones (from a High Availability Service in one zone to a VDA in a different zone) are not supported during an outage.

Local Host Cache works only with customer-deployed StoreFront. It does not work with Workspace. Local Host Cache is supported for server-hosted applications and desktops, and static (assigned) desktops.

By default, power-managed desktop VDAs in pooled Delivery Groups (created by MCS or Citrix Provisioning) that have the `ShutdownDesktopsAfterUse` property enabled are placed into maintenance mode when an outage occurs. You can change this default, to allow those desktops to be used during an outage. However, you cannot rely on the power management during the outage. (Power management resumes after normal operations resume.) Also, those desktops might contain data from the previous user, because they have not been restarted.

To override the default behavior, it must be enabled site-wide and for each affected Delivery Group. Place a support call to have it enabled site-wide (this command cannot be run using the Remote PowerShell SDK).

```powershell
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

For each affected Delivery Group, run the following PowerShell cmdlet.

```powershell
Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
```

Enabling this feature in the Site and the Delivery Groups does not affect how the configured `ShutdownDesktopsAfterUse` property works during normal operations.

**RAM size considerations**

The LocalDB service can use approximately 1.2 GB of RAM (up to 1 GB for the database cache, plus 200 MB for running SQL Server Express LocalDB). The High Availability Service can use up to 1 GB of RAM if an outage last for an extended interval with many logons occurring (for example, 12 hours with 10K users). These memory requirements are in addition to the normal RAM requirements for the Cloud Connector, so you might need to increase the total amount of RAM capacity.

**CPU core and socket configuration considerations**

A Cloud Connector’s CPU configuration, particularly the number of cores available to the SQL Server Express LocalDB, directly affects Local Host Cache performance, even more so than memory alloc-
Citrix Virtual Apps and Desktops service

This CPU overhead is observed only during the outage period when the database is unreachable and the High Availability service is active.

While LocalDB can use multiple cores (up to 4), it’s limited to only a single socket. Adding more sockets does not improve the performance (for example, having 4 sockets with 1 core each). Instead, Citrix recommends using multiple sockets with multiple cores. In Citrix testing, a 2x3 (2 sockets, 3 cores) configuration provided better performance than 4x1 and 6x1 configurations.

Storage considerations

As users access resources during an outage, the LocalDB grows. For example, during a logon/logoff test running at 10 logons per second, the database grew by 1 MB every 2-3 minutes. When normal operation resumes, the local database is recreated when a configuration change is detected. The broker must have sufficient space on the drive where the LocalDB is installed to allow for the database growth during an outage. Local Host Cache also incurs additional I/O during an outage: approximately 3 MB of writes per second, with several hundred thousand reads.

Performance considerations

During an outage, one broker handles all the connections. In resource locations that load balance among multiple Cloud Connectors during normal operations, the elected broker might need to handle many more requests than normal during an outage. Therefore, CPU demands are higher. Every broker in the resource location must be able to handle the additional load imposed by LocalDB and all of the affected VDAs, because the broker elected during an outage can change.

VDI limits:

- In a deployment with one resource location, up to 10,000 VDAs can be handled effectively during an outage.
- In a VDI deployment with more than one resource location, up to 10,000 VDAs in each resource location can be handled effectively during an outage, to a maximum of 40,000 VDAs in the deployment. For example, each of the following deployments can be handled effectively during an outage:
  - A deployment with four secondary resource locations, each containing 10,000 VDAs.
  - A deployment with seven secondary zones, one containing 10,000 VDAs, and six containing 5,000 VDAs each.

During an outage, load management may be affected. Load evaluators (and especially, session count rules) can be exceeded.

During the time it takes all VDAs to register with a broker, that broker might not have complete information about current sessions. So, a user connection request during that interval might result in
starting a new session, even though reconnection to an existing session was possible. This interval (while the new broker acquires session information from all VDAs during registration) is unavoidable. When an outage starts, connected sessions are not impacted during the transition interval, but new sessions and session reconnections can be.

This interval occurs whenever VDAs must register with a different broker:

- An outage starts: When migrating from a Brokering Principal to a secondary broker.
- Broker failure during an outage: When migrating from a secondary broker that failed to a newly elected secondary broker.
- Recovery from an outage: When normal operations resume, and the Brokering Principal resumes control.

The time it takes to synchronize between brokers increases with the number of objects (such as VDAs, applications, groups). For example, synchronizing 5000 VDAs might take ten minutes or more to complete.

**StoreFront requirement**

Each satellite zone (resource location) must have an on-premises StoreFront installed and configured. Local Host Cache works only in resource locations containing an on-premises StoreFront.

**Differences from XenApp 6.x releases**

Although this Local Host Cache implementation shares the name of the Local Host Cache feature in XenApp 6.x and earlier XenApp releases, there are significant improvements. This implementation is more robust and immune to corruption. Maintenance requirements are minimized, such as eliminating the need for periodic `dsmaint` commands. This Local Host Cache is an entirely different implementation technically.

**Manage Local Host Cache**

In a Citrix Virtual Apps and Desktops service deployment, Local Host Cache is always enabled. You don’t have to do anything else to configure or manage it.

As noted previously, the LocalDB database is installed automatically when you install a Cloud Connector in a resource location. Do not attempt to disable or remove it. (Citrix updates the Cloud Connector regularly. If you disable or remove the LocalDB software manually, the next Cloud Connector update replaces it.)
Verify that Local Host Cache is working

To verify that Local Host Cache is set up and working correctly:

- Verify that the resource location contains a local StoreFront that points to the Cloud Connectors in that resource location.
- Ensure that synchronization imports complete successfully. Check the event logs.
- Ensure that the SQL Server LocalDB was created on each Cloud Connector. This confirms that the High Availability Service can take over, if needed.
  - On the Cloud Connector server, browse to c:\Windows\ServiceProfiles\NetworkService\n  - Verify that HaDatabaseName.mdf and HaDatabaseName_logldf are created
- Force an outage on all Cloud Connectors in the resource location. After you’ve verified that Local Host Cache works, remember to place all of the Cloud Connectors back into normal mode. This can take approximately 15 minutes to avoid VDA registration storms.

See also Scalability considerations for using Local Host Cache with Cloud Connectors.

Event logs

Event logs indicate when synchronizations and outages occur.

Config Synchronizer Service:

During normal operations, the following events can occur when the CSS copies and exports the broker configuration and imports it to the LocalDB using the High Availability Service (secondary broker).

- 503: The Citrix Config Sync Service received an updated configuration. This event occurs each time the High Availability Service receives an updated configuration from Citrix Cloud. It indicates the start of the synchronization process. A 504 or 505 event always follows this event.
- 504: The Citrix Config Sync Service imported an updated configuration. The configuration import completed successfully.
- 505: The Citrix Config Sync Service failed an import. The configuration import did not complete successfully. If a previous successful configuration is available, it will be used if an outage occurs. However, it will be out-of-date from the current configuration. If there is no previous configuration available, the service cannot participate in session brokering during an outage. In this case, see the Troubleshoot section, and contact Citrix Support.
- 507: The Citrix Config Sync Service abandoned an import because the system is in outage mode and the Local Host Cache is being used for brokering. The service received a new configuration, but the import was abandoned because an outage occurred. This is expected behavior.

High Availability Service:

- 3502: An outage occurred and the secondary broker (High Availability Service) is performing broker operations.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Citrix Virtual Apps and Desktops service

- 3503: An outage was resolved and normal operations have resumed.
- 3504: Indicates which secondary broker is elected, plus other brokers involved in the election.

**Force an outage**

You might want to deliberately force an outage.

- If your network is going up and down repeatedly. Forcing an outage until the network issues are resolved prevents continuous transition between normal and outage modes (and the resulting frequent VDA registrations).
- To test a disaster recovery plan.
- To help ensure that Local Host Cache is working correctly.

To force an outage, edit the registry of each Cloud Connector server. In `HKLM\Software\Citrix\DesktopServer\LHC`, set `OutageModeForced` as `REG_DWORD` to 1. This instructs the broker to enter outage mode, regardless of the state of the connection to Citrix Cloud. Setting the value to 0 takes the broker out of outage mode. This process can take less than a minute to complete.

To verify events, monitor the `Current_HighAvailabilityService` log file in `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`.

**Troubleshoot**

Several troubleshooting tools are available when a synchronization import to the LocalDB fails and a 505 event is posted.

**CDF tracing**: Contains options for the ConfigSyncServer and BrokerLHC modules. Those options, along with other broker modules, can identify the problem.

**Report**: If a synchronization import fails, you can generate a report. This report stops at the object causing the error. This report feature affects synchronization speed, so Citrix recommends disabling it when not in use.

To enable and produce a CSS trace report, enter the command:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

The HTML report is posted at: `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`

After the report is generated, enter the following command to disable the reporting feature:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```
Scale and size considerations for Local Host Cache

October 24, 2018

Overview

The Local Host Cache feature in the Citrix Virtual Apps and Desktops service allows connection brokering in a site to continue if there is an outage. An outage happens if the WAN link between the site and the management console fails in a Citrix Cloud environment. In December 2017, we tested the Citrix Cloud Connector machine configuration using the Citrix Virtual Apps and Desktops service Local Host Cache feature. The test results provided in this document detail the tested maximums in December 2017. Best practice recommendations are based on those tested maximums.

This paper assumes that the reader can set up and configure a Citrix Cloud environment according to recommended standards, with a minimum of three Cloud Connectors.

It is important to note that Local Host Cache supports only on-premises StoreFront in each resource location or zone. In addition, Local Host Cache supports server-hosted applications and desktops and assigned desktops. Local Host Cache is not supported for pooled desktops.

While outage mode is active, if the elected connector that brokers the sessions has an outage, the second connector becomes the elected High Availability Service. After the election, the second connector takes over to broker the sessions. The Local Host Cache feature uses only one socket for multi-core CPUs for the connector VM configuration. In this scenario, we recommend a 4-core, 1-socket configuration.

Summary

All results in this summary are based on the findings from test environments which we configured as detailed in the following sections. Different system configurations yield different results.

Key recommendations based on test results

- We recommend, for high availability sites that host no more than 5,000 workstations or 500 server VDAs, that you configure 3 VMs dedicated to the Cloud Connector. Each Cloud Connector VM requires 4 vCPU with 4 GB RAM. This configuration is an N+1 high availability configuration. Cloud connectors are deployed in high availability sets. Cloud connectors are not load-balanced. Because each CPU can process a limited number of connections, the CPU is the greatest limiting factor related to the number of workstations or server VDAs supported.
- Although this document focuses on testing with two Cloud Connectors, an N+1 set of three Cloud Connectors is recommended.
We conducted session launch tests to compare Local Host Cache outage mode active and inactive after a new configuration was synchronized and imported. The launch tests covered scenarios with 5,000, 20,000, and 1,000 session launches against the respective number of available workstations.

- 5,000 sessions launched against 5,000 workstation VDAs
  * Tests used 2 Cloud Connector VMs, each had 4 vCPU and 4 GB RAM. Based on the recommendation for an N+1 configuration, production environments should include 3 Cloud Connector VMs that meet these specifications.
  * Local Host Cache service peak consumed 91% of CPU resources and there was an average of 563 MB available memory.
  * It took approximately 10 minutes from when the High Availability Service detected an outage for all VDAs to re-register with the High Availability Service, which is now the broker. We measured from the time the High Availability Service entered outage mode until the High Availability Service was ready to broker sessions again.

- 20,000 sessions launched against 500 server VDAs
  * Tests used 2 Cloud Connector VMs, each had 4 vCPU and 4 GB RAM. Based on the recommendation for an N+1 configuration, production environments should include 3 Cloud Connector VMs that meet these specifications.
  * Local Host Cache service peak consumed 90% of CPU resources and there was an average of 471 MB available memory.
  * It took approximately 8 minutes from when the High Availability Service detected an outage for all VDAs to re-register with the High Availability Service. We measured from the time the High Availability Service entered outage mode until the High Availability Service was ready to broker sessions again.

- 1,000 sessions launched against 1,000 workstation VDAs
  * Tests used 2 Cloud Connector VMs, each had 2 vCPU and 4 GB RAM. Based on the recommendation for an N+1 configuration, production environments should include 3 Cloud Connector VMs that meet these specifications.
  * Local Host Cache service peak consumed 95% of CPU resources and there was an average of 589 MB available memory.
  * It took approximately 7 minutes from when the High Availability Service detected an outage for all VDAs to re-register with the High Availability Service, which is now the broker. We measured from the time the High Availability Service entered outage mode until the High Availability Service was ready to broker sessions again.
Citrix Cloud manages Cloud Connector services, and the customer manages the machines.

**Test methodology**

We conducted tests by adding load and measuring the performance of the environment components:

- CPU
- memory
- database load
- Citrix Remote Broker Provider service
- Citrix High Availability Service

We collected performance data, logon time, or both. In certain cases, proprietary Citrix simulation tools were used to simulate VDAs and sessions. The simulation tools are designed to exercise Citrix components the same way that traditional VDAs and sessions do, without the same resource requirements to host real sessions and VDAs.

Local Host Cache supports one elected High Availability Service per zone, not per site. For example, if you have five zones, one connector is elected as the broker in each zone. The Citrix Config Synchronizer service is responsible for importing the Citrix-managed site database. Every configuration sync creates a database, so initial configurations are needed, such as compiling stored procedures the first time the database is used. We executed all tests after a configuration sync.

**Session launch tests**

On customer-managed StoreFront servers, we started 5,000 and 20,000 session tests. The monitoring tools collect StoreFront log on time, resource enumeration, and ICA file retrieval.
Citrix uses simulation tools to facilitate high-volume user testing. The simulation tools, which are proprietary to Citrix, allow us to run the tests on less hardware than is required to run tests using real sessions at these levels (5,000 and 20,000 sessions). These simulated sessions go through the normal StoreFront log on, resource enumeration, and ICA file retrieval, but do not start active desktops. Instead, the simulation tool reports to the ICA stack that the session has launched and all communication between the broker agent and the broker service is consistent with that of an actual session. Performance metrics are gathered from Citrix Cloud Connectors. To determine how the environment responded to session launches, a sustained concurrency of 25 session launches was maintained at any given time throughout the duration of the test. The measurements therefore show results of a system under load throughout the test.

Test results

Session launch

The following tables compare session launch tests between Local Host Cache outage mode active and Local Host Cache outage mode inactive after a new configuration synchronization import. Each table shows the results for the number of sessions launched in the test.

5,000 workstation VDA sessions

<table>
<thead>
<tr>
<th></th>
<th>Local Host Cache outage mode Inactive (Normal Operations) / Average Timing</th>
<th>Local Host Cache outage mode Active / Average Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>193 ms</td>
<td>95 ms</td>
</tr>
<tr>
<td>Enumerate</td>
<td>697 ms</td>
<td>75 ms</td>
</tr>
<tr>
<td>Total logon time</td>
<td>890 ms</td>
<td>170 ms</td>
</tr>
<tr>
<td>Retrieve ICA File</td>
<td>4,191 ms</td>
<td>156 ms</td>
</tr>
</tbody>
</table>

20,000 server VDA Sessions

<table>
<thead>
<tr>
<th></th>
<th>Local Host Cache outage mode Inactive (Normal Operations) / Average Timing</th>
<th>Local Host Cache outage mode Active / Average Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>135 ms</td>
<td>112 ms</td>
</tr>
<tr>
<td>Enumerate</td>
<td>317 ms</td>
<td>91 ms</td>
</tr>
</tbody>
</table>
5,000 workstation VDA session launch test
- There were approximately 30 ms of latency between the Citrix Cloud Connectors and Citrix Delivery Controller while Local Host Cache outage mode was inactive.
- There is a 720 ms difference in the logon process with Local Host Cache outage mode active versus inactive, while the StoreFront is under load.
- The largest time difference is in the retrieval of the ICA file, which is 4 seconds. This is largely because the connector is performing the brokering, whereas normally the StoreFront traffic traverses through the connectors to the Citrix Delivery Controller in Azure and back.

20,000 server VDA session launch test
- There is a 249 ms difference in the logon process with Local Host Cache outage mode active versus inactive, while the StoreFront is under load.
- The difference in the retrieval of the ICA file is about 1 second.

Compared to the 5,000-workstation VDA session launch, the 20,000-session launch test contains only 500 server VDAs, resulting in fewer calls from the Citrix Delivery Controller to the VDAs, which leads to lower response times.

### Average CPU usage comparison

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average CPU %</th>
<th>Peak CPU %</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>Connector 1</td>
<td>8.3</td>
</tr>
<tr>
<td></td>
<td>Connector 2</td>
<td>8.4</td>
</tr>
<tr>
<td>5,000 workstation VDA sessions - Local Host Cache outage mode active</td>
<td>Connector 1 (elected High Availability Service)</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Connector 2</td>
<td>0.8</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>Connector 1</td>
<td>23</td>
</tr>
</tbody>
</table>
### Session launch test

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average CPU %</th>
<th>Peak CPU %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector 2</td>
<td>23</td>
<td>55</td>
</tr>
<tr>
<td>20,000 server VDA sessions - Local Host Cache outage mode active</td>
<td>Connector 1 (elected High Availability Service)</td>
<td>57</td>
</tr>
<tr>
<td>Connector 2</td>
<td>0.8</td>
<td>6.6</td>
</tr>
</tbody>
</table>

- The table compares Citrix Cloud Connector CPU usage with Local Host Cache outage mode active and Local Host Cache mode inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.
- All Cloud Connectors are 4 vCPU and 4 GB RAM
- The elected High Availability Service machines peaked at 91% and 90% overall CPU respectively. It is worth noting that, while the non-elected High Availability Service does not have much usage, it may become the active if the elected High Availability Service has a failure. It is therefore critical for the connectors to have identical connector specifications.

### Available memory usage

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average Available Memory (working set MB)</th>
<th>Peak Available Memory (working set MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>Connector 1</td>
<td>636</td>
</tr>
<tr>
<td></td>
<td>Connector 2</td>
<td>786</td>
</tr>
<tr>
<td>5,000 workstation VDA sessions - Local Host Cache outage mode active</td>
<td>Connector 1 (elected High Availability Service)</td>
<td>563</td>
</tr>
<tr>
<td></td>
<td>Connector 2</td>
<td>912</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>Connector 1</td>
<td>1030</td>
</tr>
<tr>
<td></td>
<td>Connector 2</td>
<td>1178</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average Available Memory (working set MB)</th>
<th>Peak Available Memory (working set MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20,000 server VDA sessions - Local Host Cache outage mode active</td>
<td>Connector 1 (elected High Availability Service)</td>
<td>471</td>
</tr>
<tr>
<td></td>
<td>Connector 2</td>
<td>1210</td>
</tr>
</tbody>
</table>

- The table compares available memory usage with Local Host Cache outage mode active and Local Host Cache mode inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.
- The number of sessions decreases the amount of available memory.
- There is a 54.35% (559 MB) increase in memory usage with 20,000 server VDA sessions when Local Host Cache outage mode is active, mainly due to SQL server memory consumption.

Cloud Connector CPU usage by component

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Component</th>
<th>Average CPU %</th>
<th>Peak CPU %</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>Connector 1 LSASS</td>
<td>2.4</td>
<td>10.7</td>
</tr>
<tr>
<td></td>
<td>Connector 1 XaXdCloudProxy</td>
<td>3.5</td>
<td>18.5</td>
</tr>
<tr>
<td></td>
<td>Connector 2 LSASS</td>
<td>2.5</td>
<td>12.9</td>
</tr>
<tr>
<td></td>
<td>Connector 2 XaXdCloudProxy</td>
<td>3.5</td>
<td>21.2</td>
</tr>
<tr>
<td>5,000 workstation VDA sessions Local Host Cache outage mode active</td>
<td>Connector 1 (elected High Availability Service) LSASS</td>
<td>12.9</td>
<td>29.5</td>
</tr>
<tr>
<td></td>
<td>Connector 1 (elected High Availability Service) HighAvailabilityService</td>
<td>14.7</td>
<td>49.7</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>Connector 1 LSASS</td>
<td>7</td>
<td>12.2</td>
</tr>
<tr>
<td>Session launch test</td>
<td>Component</td>
<td>Average CPU %</td>
<td>Peak CPU %</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------</td>
<td>---------------</td>
<td>------------</td>
</tr>
<tr>
<td>Connector 1</td>
<td>XaXdCloudProxy</td>
<td>8.7</td>
<td>15.5</td>
</tr>
<tr>
<td>Connector 2</td>
<td>LSASS</td>
<td>7</td>
<td>12.5</td>
</tr>
<tr>
<td>20,000 sessions Local Host Cache outage mode active</td>
<td>Connector 1 (elected High Availability Service) LSASS</td>
<td>4.3</td>
<td>17.2</td>
</tr>
<tr>
<td></td>
<td>Connector 1 (elected High Availability Service) High Availability Service</td>
<td>4.5</td>
<td>18.2</td>
</tr>
</tbody>
</table>

- The preceding table shows the processes that consume the most overall CPU resources when Local Host Cache outage mode is active, compared to when Local Host Cache outage mode is inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.
- The Citrix Remote Broker Provider service (XaXdCloudProxy) is the top CPU consumer when Local Host Cache outage mode is inactive.
- LSASS (Local Security Authority Subsystem Service) uses CPU during session logons. All authentications from Citrix-managed services must traverse the Citrix Cloud Connectors to communicate with the customer-managed Active Directory.
- The Citrix High Availability Service is used to broker the sessions, resulting in higher CPU usage when Local Host Cache outage mode is active. Also, CPU usage peaked to 49.7% during the 5,000 workstation VDA session launch, while the usage was only 18.25% during the 20,000 server VDA session launch (500 VDAs). The difference is due to the number of VDAs.
- Connector 2 did not have any meaningful metrics, as it was not the elected High Availability Service.

**VDA re-registration time while switching to Local Host Cache**

During a Delivery Controller outage, the 5,000 workstation VDAs must re-register with the elected Local Host Cache broker. This re-registration time was ~10 minutes. The re-registration time for 500 server VDAs was ~8 minutes.
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Number of VDAs</th>
<th>Re-Registration time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDAs</td>
<td>~10 minutes</td>
</tr>
<tr>
<td>500 server VDAs</td>
<td>~8 minutes</td>
</tr>
</tbody>
</table>

**Outage timings**

<table>
<thead>
<tr>
<th>Outage event</th>
<th>Number of VDAs</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter outage mode</td>
<td></td>
<td>10 minutes</td>
</tr>
<tr>
<td>Re-registration time to elected High Availability Service</td>
<td>500</td>
<td>~8 minutes</td>
</tr>
<tr>
<td></td>
<td>5000</td>
<td>~10 minutes</td>
</tr>
<tr>
<td>Exit outage mode</td>
<td></td>
<td>10 minutes</td>
</tr>
<tr>
<td>Re-registration time to Citrix Delivery Controller</td>
<td>500</td>
<td>~5.5 minutes</td>
</tr>
<tr>
<td></td>
<td>5000</td>
<td>~1.5 minutes</td>
</tr>
</tbody>
</table>

- There is a total of 20 minutes to enter (10 minutes) and exit (10 minutes) outage mode, due to the number of Citrix Delivery Controller health checks required. The time required to re-register the VDAs adds to the overall outage time.
- If the network is going up and down repeatedly, forcing an outage until the network issues resolve prevents continuous transition between normal and outage modes.

**Database and High Availability Service metrics with Local Host Cache**

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average High Availability Service Database Transactions/sec</th>
<th>Peak High Availability Service Database Transactions/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>436</td>
<td>1344</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>590</td>
<td>2061</td>
</tr>
</tbody>
</table>

The preceding table shows the number of database transactions per second on the elected High Avail-
ability Service.

**StoreFront CPU usage comparison**

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average CPU %</th>
<th>Peak CPU %</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>4.5</td>
<td>32.4</td>
</tr>
<tr>
<td>5,000 server VDA sessions</td>
<td>13.8</td>
<td>32.6</td>
</tr>
<tr>
<td>Local Host Cache outage mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>11.4</td>
<td>22.1</td>
</tr>
<tr>
<td>20,000 server VDA sessions - Local Host Cache outage mode</td>
<td>18.6</td>
<td>33.2</td>
</tr>
</tbody>
</table>

- The preceding table compares StoreFront CPU usage when Local Host Cache outage mode is active to when Local Host Cache mode is inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.
- The StoreFront machine has the following specifications: Windows 2012 R2, 8 vCPU (2 sockets, 4 cores each), 8 GB RAM.
- When Local Host Cache outage mode is active, there is approximately a 9% increase in average CPU usage with the 5,000 workstation VDA and about a 7% increase with the 20,000 server VDA session launch tests. The increase is mostly because the IIS worker processes more requests when Local Host Cache outage mode is active. There is more CPU usage because StoreFront is processing session launches at a faster rate than when outage mode is inactive.

**StoreFront available memory usage comparison**

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average Available Memory (working set MB)</th>
<th>Peak Available Memory (working set MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000 workstation VDA sessions</td>
<td>5731</td>
<td>6821</td>
</tr>
<tr>
<td>5,000 workstation VDA sessions Local Host Cache outage mode</td>
<td>5345</td>
<td>5420</td>
</tr>
<tr>
<td>20,000 server VDA sessions</td>
<td>4671</td>
<td>4924</td>
</tr>
</tbody>
</table>
The preceding table compares the StoreFront available memory usage when Local Host Cache outage mode is active and when Local Host Cache mode is inactive during 5,000 workstation VDA and 20,000 server VDA session launch tests.

- When Local Host Cache mode is active, there is a 6.73% increase in memory usage during the 5,000 workstation VDA session launch test.

The following table compares outage mode active vs inactive after a new configuration synchronization import, launching 1,000 sessions to 1,000 workstation VDAs with Local Host Cache, and using Citrix Cloud Connectors configured with 2 vCPU VMs.

### Session launch comparison

<table>
<thead>
<tr>
<th></th>
<th>Local Host Cache outage mode inactive (normal operations)</th>
<th>Local Host Cache outage mode active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>359 ms</td>
<td>89 ms</td>
</tr>
<tr>
<td>Enumerate</td>
<td>436 ms</td>
<td>180 ms</td>
</tr>
<tr>
<td>Total logon time</td>
<td>795 ms</td>
<td>269 ms</td>
</tr>
<tr>
<td>Retrieve ICA File</td>
<td>804 ms</td>
<td>549 ms</td>
</tr>
</tbody>
</table>

- While the StoreFront in under load, there is a 526 ms difference in the logon process when Local Host Cache outage mode is active compared to when Local Host Cache mode is inactive.
- There is a 255 ms difference in the retrieval of the ICA file when Local Host Cache outage mode is active compared to when Local Host Cache mode is inactive. The difference increases with the number of sessions.

### Average CPU usage comparison

© 1999-2019 Citrix Systems, Inc. All rights reserved.
The elected High Availability Service peaked to 95% overall CPU, which indicates that 1,000 workstation VDA is an optimal configuration for a 2 vCPU connector VM.

**Average memory usage comparison**

The preceding graph displays a comparison of Citrix Cloud Connector available usage when Local Host
Cache outage mode is active versus inactive, during a 1,000 workstation VDA session launch. There is not a significant difference in memory based on the Local Host Cache outage mode.

**Cloud Connector CPU usage by component comparison**

The preceding graph displays the processes that consume the most CPU resources while Local Host Cache outage mode is inactive.
• The preceding graph displays the processes that consume the most CPU resources when Local Host Cache outage mode is active.
• Connector 2 did not have any meaningful metrics.

**VDA re-registration time while switching to Local Host Cache**

During a Delivery Controller outage, the 1000 workstation VDAs must re-register with the elected Local Host Cache broker. The re-registration time was ~7 minutes.

**Database and High Availability Service metrics with Local Host Cache**
The preceding graph displays the number of database transactions per second on the elected High Availability Service.

**Impact with increasing number of zones on database import times**

An extra zone (with a pair of its own connectors) was added to the test site to understand the impact. The first zone consists of 5,500 unique objects (2 catalogs). The secondary zone is a mirror of the first zone, and has its own unique objects, totaling 11,000 objects. It is important to note that Local Host Cache is recommended only for zones with no more than 10,000 objects. Before we added the secondary zone, database import time on the connectors was about 4 minutes, 20 seconds. After we added the secondary zone and populated it with 11,000 objects, the import time increased to by ~30 seconds to ~4 minutes, 50 seconds. Adding more catalogs has marginal impact on import times. The largest contributing factors to performance degradation and increased import times are based on the number of assigned machines, users, and remote PCs. Additionally, 5,500 objects were split between 2 zones and the import time remained the same.

<table>
<thead>
<tr>
<th>Number of zones</th>
<th>Total Number of Objects</th>
<th>Import time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5,500</td>
<td>4 minutes 20 seconds</td>
</tr>
<tr>
<td>2</td>
<td>11,000</td>
<td>4 minutes 50 seconds</td>
</tr>
<tr>
<td>2</td>
<td>5,500</td>
<td>4 minutes 20 seconds</td>
</tr>
</tbody>
</table>
**Connector Sizing Guidance**

For optimal performance, the following are the recommended configurations for Citrix Cloud Connector when Local Host Cache mode is enabled.

**Recommendation 1:** to support 1,000 workstation VDAs using Local Host Cache mode with Citrix Cloud Connector

- 2 Windows 2012 R2 VMs, each allocated with 2 vCPU (1 socket, 2 cores), 4 GB RAM
- This recommended sizing is based on the peak Citrix Cloud Connector overall 95% CPU usage and 589 MB average available memory while Local Host Cache mode is active

**Recommendation 2:** to support 5,000 workstation VDAs OR 500 server VDAs using Local Host Cache with Citrix Cloud Connector

- 2 Windows 2012 R2 VMs, each allocated with 4 vCPU (1 socket, 4 cores), 4 GB RAM
- This recommended sizing is based on
  - 5,000 workstation VDA sessions launched with Local Host Cache mode active
    * Overall 91% peak CPU usage
    * 563 MB average available memory
  - 20,000 server VDA sessions launched with Local Host Cache mode active
    * Overall 90% peak CPU usage
    * 471 MB average available memory

See the white paper Citrix Cloud Virtual Apps and Desktops service sizing and scalability considerations for more information about general scalability sizing.

**Test environment**

The test environment employed internally developed, proprietary testing tools, and VMs configured to the specifications in the following sections.

**Tools used**

We used an internal testing tool to collect performance data and metrics from the machines under test and to drive the session launches. The in-house testing tool orchestrates user session launches to the Citrix Virtual Apps and Desktops environment. The testing tool also provides a central location where we gather response time data and performance metrics. In essence, the test tool administers the tests and collects the results.

**Test configuration – Citrix Virtual Apps and Desktops service**

The following is a list of the machine and OS specifications used with the Citrix Virtual Apps and Desktops service testing.
Citrix Virtual Apps and Desktops service

- **Cloud Connectors:**
  - 2 Windows 2012 R2 VMs, each allocated 4 vCPU (1 socket, 4 cores), 4 GB RAM
  - 2 Windows 2012 R2 VMs, each allocated 2 vCPU (1 socket, 2 cores), 4 GB RAM
- **StoreFront (Customer-managed):** Windows 2012 R2, 8 vCPU (2 sockets, 4 cores each), 8 GB RAM
- **Hypervisor:** Citrix XenServer 7.0 + updates, 5x HP Blade BL 460C Gen 9, 2x Intel E5-2620 CPU, 256 GB RAM
- **Hypervisor Storage:** 2 TB NFS share on NetApp 3250
- **VDA:** Windows 2012 R2

**Data Collection**

We collect the following metrics from each test: average overall CPU, memory, component (cloud processes) usage increase.

- VDA re-registration time when switching to the elected Local Host Cache High Availability Service
- Database and High Availability Service metrics when Local Host Cache outage mode is active
- Session launch comparison, average timings for
  - Authentication
  - Enumeration
  - ICA file retrieval
- Impact to database synchronization times while increasing the number of zones
  - Time required to synchronize after a configuration change

**Tags**

September 18, 2019

**Introduction**

Tags are strings that identify items such as machines, applications, desktops, Delivery Groups, Application Groups, and policies. After creating a tag and adding it to an item, you can tailor certain operations to apply to only items that have a specified tag.

- Tailor search displays in Studio.

  For example, to display only applications that have been optimized for testers, create a tag named “test” and then add (apply) it to those applications. You can now filter the Studio search with the tag “test”.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
• Publish applications from an Application Group or specific desktops from a Delivery Group, considering only a subset of the machines in selected Delivery Groups. This is called a *tag restriction*.

With tag restrictions, you can use your existing machines for more than one publishing task, saving the costs associated with deploying and managing additional machines. A tag restriction can be thought of as subdividing (or partitioning) the machines in a Delivery Group. Its functionality is similar, but not identical, to worker groups in XenApp releases earlier than 7.x.

Using an Application Group or desktops with a tag restriction or can be helpful when isolating and troubleshooting a subset of machines in a Delivery Group.

See below for details and examples of using a tag restriction.

• Schedule periodic restarts for a subset of machines in a Delivery Group.

Using a tag restriction for machines enables you to use new PowerShell cmdlets to configure multiple restart schedules for subsets of machines in a Delivery Group. For examples and details, see [Manage Delivery Groups](#).

• Tailor the application (assignment) of Citrix policies to a subset of machines in Delivery Groups, Delivery Group types, or OUs that have (or do not have) a specified tag.

For example, if you want to apply a Citrix policy only to the more powerful workstations, add a tag named “high power” to those machines. Then, on the **Assign Policy** page of the Create Policy wizard, select that tag and also the **Enable** checkbox. You can also add a tag to a Delivery Group and then apply a Citrix policy to that group. For details, see Create policies and this [blog post](#). (The Studio interface for adding a tag to a machine has changed since the blog post was published.)

You can apply tags to:

• Machines
• Applications
• Delivery Groups
• Application Groups

You can configure a tag restriction can be configured when creating or editing the following in Studio:

• A desktop in a shared Delivery Group
• An Application Group

**Tag restrictions for a desktop or an Application Group**

A tag restriction involves several steps:

• Create the tag and then add (apply) it to machines.
• Create or edit a group with the tag restriction (in other words, “restrict launches to machines with tag x”).

A tag restriction extends the broker’s machine selection process. The broker selects a machine from an associated Delivery Group subject to access policy, configured user lists, zone preference, and launch readiness, plus the tag restriction (if present). For applications, the broker falls back to other Delivery Groups in priority order, applying the same machine selection rules for each considered Delivery Group.

**Example 1: Simple layout**

This example introduces a simple layout that uses tag restrictions to limit which machines will be considered for certain desktop and application launches. The site has one shared Delivery Group, one published desktop, and one Application Group configured with two applications.

• Tags have been added to each of the three machines (VDA 101-103).
• The desktop in the shared Delivery Group was created with a tag restriction named “Red,” so that desktop can be launched only on machines in that Delivery Group that have the tag “Red”: VDA 101 and 102.
• The Application Group was created with the “Orange” tag restriction, so each of its applications (Calculator and Notepad) can be launched only on machines in that Delivery Group that have the tag “Orange”: VDA 102 and 103.

Machine VDA 102 has both tags (Red and Orange), so it can be considered for launching the applications and the desktop.

**Example 2: More complex layout**

This example contains several Application Groups that were created with tag restrictions. This results in the ability to deliver more applications with fewer machines than would otherwise be needed if you used only Delivery Groups.

How to configure example 2 shows the steps used to create and apply the tags, and then configure the tag restrictions in this example.

This example uses ten machines (VDA 101-110), one Delivery Group (D01), and three Application Groups (A100, A200, A300). By applying tags to each machine and then specifying tag restrictions when creating each Application Group:

• Accounting users in the group can access the apps they need on five machines (VDA 101–105)
• CAD designers in the group can access the apps they need on five machines (VDA 106-110)
• Users in the group who need Office applications can access the Office apps on ten machines (VDA 101-110)
Only ten machines are used, with only one Delivery Group. Using Delivery Groups alone (without Application Groups) would require twice as many machines, because a machine can belong to only one Delivery Group.

**Manage tags and tag restrictions**

Tags are created, added (applied), edited, and deleted from selected items through the Manage Tags action in Studio.

(Exception: Tags used for policy assignments are created, edited, and deleted through the Manage Tags action in Studio; however, tags are applied (assigned) when you create the policy. See Create policies for details.)

Tag restrictions are configured when you create or edit desktops in Delivery Groups, and when you create and edit Application Groups.

**Use the Manage Tags dialogs in Studio**

In Studio, select the items you want to apply a tag to (one or more machines, applications, a desktop, a Delivery Group, or an Application Group) and then select Manage Tags in the Actions pane. The Manage Tags dialog box lists all the tags that have been created in the Site, not just for the items you selected.

- A check box containing a check mark indicates that tag has already been added to the selected items. (In the screen capture below, the selected machine has the tag named “Tag1” applied.)
- If you selected more than one item, a check box containing a hyphen indicates that some, but not all selected items have that tag added.

The following actions are available from the Manage Tags dialog box. Be sure to review Cautions when working with tags.

- **To create a tag:**
  
  Click Create. Enter a name and description. Tag names must be unique and are not case-sensitive. Then click OK. (Creating a tag does not automatically apply it to any items you have selected. Use the check boxes to apply the tag.)

- **To add (apply) one or more tags:**
  
  Enable the check box next to the tag name. If you selected multiple items and the check box next to a tag contains a hyphen (indicating that some, but not all selected items already have the tag applied), changing it to a check mark affects all of the selected machines.
If you attempt to add a tag to one or more machines, and that tag is currently used as a restriction in an Application Group, you are warned that the action can result in making those machines available for launch. If that’s what you intended, proceed.

- **To remove one or more tags:**
  Clear the check box next to the tag name. If you selected multiple items and the check box next to a tag contains a hyphen (indicating that some, but not all selected items already have the tag applied), clearing the check box removes the tag from all of the selected machines.

  If you attempt to remove a tag from a machine that is using that tag as a restriction, you are warned that the action can affect which machines are considered for launch. If that’s what you intended, proceed.

- **To edit a tag:**
  Select a tag and then click **Edit**. Enter a new name and/or description. You can edit only one tag at a time.

- **To delete one or more tags:**
  Select the tags and then click **Delete**. The Delete Tag dialog box indicates how many items currently use the selected tags (for example “2 machines”). Click an item to display more information. For example, clicking a “2 machines” item displays the names of the two machines that have that tag applied. Confirm whether you want to delete the tags.

  You cannot use Studio to delete a tag that is used as a restriction. You must first edit the Application Group and remove the tag restriction or select a different tag.

When you’re done in the Manage Tags dialog box, click **Save**.

To see if a machine has any tags applied: Select **Delivery Groups** in the navigation pane. Select a Delivery Group in the middle pane and then select **View Machines** in the Actions pane. Select a machine in the middle pane and then select the Tags tab on the Details pane below.

### Manage tag restrictions

Configuring a tag restriction is a multi-step process: You first create the tag and add/apply it to machines. Then, you add the restriction to the Application Group or the desktop.

- **Create and apply the tag:**
  Create the tag and then add (apply) it to the machines that will be affected by the tag restriction, using the **Manage Tags** actions described above.

- **To add a tag restriction to an Application Group:**
  Create or edit the Application Group. On the Delivery Groups page, select **Restrict launches to machines with the tag** and then select the tag from the dropdown.
• **To change or remove the tag restriction on an Application Group:**
   Edit the group. On the Delivery Groups page, either select a different tag from the dropdown or remove the tag restriction entirely by clearing **Restrict launches to machines with the tag**.

• **To add a tag restriction to a desktop:**
   Create or edit a Delivery Group. Click **Add** or **Edit** on the **Desktops** page. In the Add Desktop dialog box, select **Restrict launches to machines with the tag** and then select the tag from the menu.

• **To change or remove the tag restriction on a Delivery Group:**
   Edit the group. On the Desktops page, click **Edit**. In the dialog box, either select a different tag from the dropdown or remove the tag restriction entirely by clearing **Restrict launches to machines with the tag**.

**Cautions when working with tags**

A tag applied to an item can be used for different purposes, so keep in mind that adding, removing, and deleting a tag can have unintended effects. You can use a tag to sort machine displays in the Studio search field. You can use the same tag as a restriction when configuring an Application Group or a desktop, which will limit launch consideration to only machines in specified Delivery Groups that have that tag.

If you attempt to add a tag to one or more machines after that tag has been configured as a tag restriction for a desktop or an Application Group, Studio warns you that adding that tag might make the machines available for launching additional applications or desktops. If that is what you intended, proceed. If not, you can cancel the operation.

For example, let’s say you create an Application Group with the “Red” tag restriction. Later, you add several other machines in the same Delivery Groups used by that Application Group. If you then attempt to add the “Red” tag to those machines, Studio will display a message similar to: “The tag “Red” is used as a restriction on the following Application Groups. Adding this tag might make the selected machines available to launch applications in this Application Group.” You can then confirm or cancel adding that tag to those additional machines.

Similarly, if a tag is being used in an Application Group to restrict launches, Studio warns that you cannot delete the tag until you remove it as a restriction by editing the group. (If you were allowed to delete a tag that’s used as a restriction in an Application Group, that could result in allowing applications to launch on all machines in the Delivery Groups associated with the Application Group.) The same prohibition against deleting a tag applies if the tag is currently being used as a restriction for desktop launches. After you edit the Application Group or desktops in the Delivery Group to remove that tag restriction, you can delete the tag.
Citrix Virtual Apps and Desktops service

All machines may not have the same sets of applications. A user may belong to more than one Application Group, each with a different tag restriction and different or overlapping sets of machines from Delivery Groups. The following table lists how machine considerations are decided.

<table>
<thead>
<tr>
<th>When an application has been added to</th>
<th>These machines in the selected Delivery Groups are considered for launch</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Application Group with no tag restriction</td>
<td>Any machine</td>
</tr>
<tr>
<td>One Application Group with tag restriction A</td>
<td>Machines that have tag A applied</td>
</tr>
<tr>
<td>Two Application Groups, one with tag restriction A and the other with tag restriction B</td>
<td>Machines that have tag A and tag B; if none are available, then machines that have tag A or tag B</td>
</tr>
<tr>
<td>Two Application Groups, one with tag restriction A and the other with no tag restriction</td>
<td>Machines that have tag A; if none are available, then any machine</td>
</tr>
</tbody>
</table>

If you used a tag restriction in a machine restart schedule, any changes you make that affect tag applications or restrictions affect the next machine restart cycle. It does not affect any restart cycles that is in progress while the changes are being made.

**How to configure example 2**

The following sequence shows the steps to create and apply tags, and then configure tag restrictions for the Application Groups illustrated in the second example above.

VDAs and applications have already been installed on the machines and the Delivery Group has been created.

Create and apply tags to the machines:

1. In Studio, select Delivery Group D01 and then select **View Machines** in the Action pane.
2. Select machines VDA 101-105 and then select **Manage Tags** in the Actions pane.
3. In the Manage Tags dialog box, click **Create** and then create a tag named CADApps. Click **OK**.
4. Click **Create** again and create a tag named OfficeApps. Click **OK**.
5. While still in the Manage Tags dialog box, add (apply) the newly-created tags to the selected machines by enabling the check boxes next to each tag’s name (CADApps and OfficeApps), and then close the dialog box.
6. Select Delivery Group D01, select **View Machines** in the Action pane.
7. Select machines VDA 106-110 and then select **Manage Tags** in the Actions pane.
8. In the Manage Tags dialog box, click **Create** and then create a tag named AcctgApps. Click **OK**.
9. Apply the newly-created AcctgApps tag and the OfficeApps tag to the selected machines by clicking the check boxes next to each tag’s name, and then close the dialog box.

Create the Application Groups with tag restrictions.

1. In Studio, select Applications in the navigation pane and then select Create Application Group in the Actions pane. The Create Application Group wizard launches.
2. On the Delivery Groups page of the wizard, select Delivery Group D01. Select Restrict launches to machines with tag and then select the AcctgApps tag from the dropdown.
3. Complete the wizard, specifying the accounting users and the accounting applications. (When adding the application, choose the “From Start menu” source, which will search for the application on the machines that have the AcctgApps tag.) On the Summary page, name the group A100.
4. Repeat the preceding steps to create Application Group A200, specifying machines that have the CADApps tag, plus the appropriate users and applications.
5. Repeat steps to create Application Group A300, specifying machines that have the OfficeApps tag, plus the appropriate users and applications.

Tags on machine catalogs

Important:
This feature is being rolled out in phases. It might not yet be activated for your account.

You can use tags on machine catalogs. The overall sequence of creating a tag and then applying it to a catalog is the same as described previously. However, applying tags to catalogs is supported only through the PowerShell interface. You cannot use Studio to apply a tag to a catalog or remove a tag from a catalog. Catalog displays in Studio do not indicate if a tag is applied.

Summary: You can use Studio or PowerShell to create or delete a tag for use on a catalog. You must use PowerShell to apply the tag to the catalog.

Here are some examples of using tags with catalogs:

- A Delivery Group has machines from several catalogs, but you want an operation (such as a restart schedule) to affect only the machines in a specific catalog. Applying a tag to that catalog accomplishes that.
- In an Application Group, you want to limit application sessions to machines in a specific catalog. Applying a tag to that catalog accomplishes that.

Affected PowerShell cmdlets:

- You can pass catalog objects to cmdlets such as Add-BrokerTag and Remove-BrokerTag.
- Get-BrokerTagUsage shows how many catalogs contain tags.
- Get-BrokerCatalog has a property named Tags.
For example, the following cmdlets add a tag named `fy2018` to the catalog named `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`. (The tag was previously created using either Studio or PowerShell.)

See the PowerShell cmdlet help for additional guidance and syntax.

**More information**

The blog post [How to assign desktops to specific servers](#) also links to the following video.

---

**Zones**

September 27, 2019
Introduction

Citrix Virtual Apps and Desktops service deployments that span widely dispersed locations connected by a WAN can face challenges from network latency and reliability. Using zones can help users in remote regions connect to resources without necessarily forcing their connections to traverse large segments of the WAN. In a Citrix Virtual Apps and Desktops service environment, each resource location is considered a zone.

Zones can be helpful in deployments of all sizes. You can use zones to keep applications and desktops closer to users, which improves performance. Zones can be used for disaster recovery, geographically distant data centers, branch offices, a cloud, or an availability zone in a cloud.

Throughout this article, the term local refers to the zone being discussed. For example, “A VDA registers with a local Cloud Connector” means that a VDA registers with a Cloud Connector in the zone where the VDA is located.

Differences from zones in on-premises Citrix Virtual Apps and Desktops environments

Zones in a Citrix Virtual Apps and Desktops service environment are similar, but not identical to zones in an on-premises Citrix Virtual Apps and Desktops deployment.

- In the Citrix Virtual Apps and Desktops service, zones are created automatically when you create a resource location and add a Cloud Connector to it. Unlike an on-premises deployment, a service environment does not classify zones as primary or satellite.
- In XenApp version 6.5 and earlier, zones included data collectors. The Citrix Virtual Apps and Desktops service does not use data collectors for zones. Also, failover and preferred zones work differently.

What’s in a zone

A zone is equivalent to a resource location. When you create a resource location and install a Cloud Connector, a zone is automatically created for you. Each zone can have a different set of resources, based on your unique needs and environment.
Each zone must always have at least one Cloud Connector, and preferably two or more, for redundancy.

You can place machine catalogs, hypervisors, host connections, users, and applications in a zone. A zone can also contain Citrix Gateway and StoreFront servers. To use the Local Host Cache feature, a zone must have a StoreFront server. For more information, see Resource types.

Zones work with the Citrix Cloud workspace experience and the Citrix Gateway Service.

Placing items in a zone affects how the service interacts with them and with other objects related to them.

- When a hypervisor connection is placed in a zone, it is assumed that all the hypervisors managed through that connection also reside in that zone.
- When a machine catalog is placed in a zone, it is assumed that all VDAs in the catalog are in the zone.
- Citrix Gateway instances can be added to zones. When you create a resource location, you are offered the option to add a Citrix Gateway. When a Citrix Gateway is associated with a zone, it is preferred for use when connections to VDAs in that zone are used.
- Ideally, Citrix Gateway in a zone is used for user connections coming into that zone from other zones or external locations. You can also use it for connections within the zone.
- After you create more resource locations and install Cloud Connectors in them (which automatically creates more zones), you can move resources between zones. This flexibility comes with the risk of separating items that work best in close proximity. For example, moving a catalog to a different zone than the connection (host) that creates the machines in the catalog, can affect performance. So, consider potential unintended effects before moving items between zones. Keep a catalog and the host connection it uses in the same zone.
If the connection between a zone and Citrix Cloud fails, the Local Host Cache feature enables a Cloud Connector in the zone to continue brokering connections to VDAs in that zone. (The zone must have StoreFront installed.) For example, this is effective in an office where workers use the local StoreFront site to access their local resources, even if the WAN link connecting their office to the corporate network fails. For more information, see Local Host Cache.

**Where VDAs register**

VDAs must be minimum version 7.7 to use these zone registration features:

- A VDA in a zone registers with a local Cloud Connector.
  - As long as that Cloud Connector can communicate with Citrix Cloud, normal operations continue.
  - If that Cloud Connector is operational but cannot communicate with Citrix Cloud (and that zone has a local StoreFront), it enters Local Host Cache outage mode.
  - If a Cloud Connector fails, VDAs in that zone attempt to register with other local Cloud Connectors. A VDA in one zone never attempts to register with a Cloud Connector in another zone.
- If you add or remove a Cloud Connector in a zone (using the Citrix Cloud management console), and auto-update is enabled, VDAs in that zone receive updated lists of available local Cloud Connectors, so they know with whom they can register and accept connections from.
- If you move a machine catalog to another zone (using Studio), the VDAs in that catalog re-register with Cloud Connectors in the zone where you moved the catalog. When you move a catalog, ensure you also move any associated host connection to the same zone.
- During an outage (when Cloud Connectors in a zone cannot communicate with Citrix Cloud), only the resources associated with machines that are registered in that zone are available.

**Zone preference**

In a multi-zone Site, the zone preference feature offers the administrator more flexibility to control which VDA is used to launch an application or desktop.

**How zone preference works**

There are three forms of zone preference. You might prefer to use a VDA in a particular zone, based on:

- Where the application’s data is stored. This is referred to as the application home.
- The location of the user’s home data, such as a profile or home share. This is referred to as the user home.
• The user’s current location (where the Citrix Workspace app is running). This is referred to as the user location. User location requires minimum StoreFront 3.7 and Citrix Gateway (formerly NetScaler Gateway) 11.0-65.x.

The following graphic shows an example multi-zone configuration.

In this example, VDAs are spread among three zones, but they are all in the same Delivery Group. Therefore, the Citrix Virtual Apps and Desktops service broker might have a choice which VDA to use for a user launch request. This example illustrates that users can be running their Citrix Workspace app endpoints at different locations. User A is using a device with Citrix Workspace app in zone 1. User B is using a device in zone 2. Similarly, a user’s documents can be stored in different locations. Users A and B use a share located in zone 1; User C uses a share in zone 3. Also, one of the published applications uses a database located in zone 1.

You associate a user or application with a zone by configuring a home zone for the user or application. The broker then uses those associations to help select the zone where a session will be launched, if resources are available. You:

• Configure the home zone for a user by adding a user to a zone.
• Configure the home zone for an application by editing the application’s properties.

A user or an application can have only one home zone at a time. (An exception for users can occur when multiple zone memberships occur because of user group membership. However, even in this
case, the broker uses only one home zone.)

Although zone preferences for users and applications can be configured, the broker selects only one preferred zone for a launch. The default priority order for selecting the preferred zone is: application home > user home > user location. When a user launches an application:

- If that application has a configured zone association (an application home), then the preferred zone is the home zone for that application.
- If the application does not have a configured zone association, but the user has a configured zone association (a user home), then the preferred zone is the home zone for that user.
- If neither the application nor the user has a configured zone association, then the preferred zone is the zone where the user is running a Citrix Workspace app instance (the user location). If that zone is not defined, a random VDA and zone selection is used. Load balancing is applied to all VDAs in the preferred zone. If there is no preferred zone, load balancing is applied to all VDAs in the Delivery Group.

**Tailoring zone preference**

When you configure (or remove) a home zone for a user or an application, you can also further restrict how zone preference is (or is not) used.

- **Mandatory user home zone use:** In a Delivery Group, you can specify “launch the session in the user’s home zone (if the user has a home zone), with no failover to a different zone if resources are not available in the home zone.” This restriction is helpful if you want to avoid the risk of copying large profiles or data files between zones. In other words, you would rather deny a session launch than launch the session in a different zone.
- **Mandatory application home zone use:** Similarly, when you configure a home zone for an application, you can specify “launch the application only in that zone, with no failover to a different zone if resources are not available in the application’s home zone.”
- **No application home zone, and ignore configured user home zone:** If you do not specify a home zone for an application, you can also specify “do not consider any configured user zones when launching that application.” For example, use the user location zone preference if you want users to run a specific application on a VDA close to their machine, even though some users might have a different home zone.

**How preferred zones affect session use**

When a user launches an application or desktop, the broker prefers using the preferred zone rather than using an existing session.

If the user launching an application or desktop already has a session that is suitable for the resource being launched (for example, that can use session sharing for an application, or a session that is al-
ready running the resource being launched), but that session is running on a VDA in a zone other than the preferred zone for the user/application, then the system may create a new session. This satisfies launching in the correct zone (if it has available capacity), ahead of reconnecting to a session in a less-preferred zone for that user’s session requirements.

To prevent an orphan session that can no longer be reached, reconnection is allowed to existing disconnected sessions, even if they are in a non-preferred zone.

The order of desirability for sessions to satisfy a launch is:

1. Reconnect to an existing session in the preferred zone.
2. Reconnect to an existing disconnected session in a non-preferred zone.
3. Start a new session in the preferred zone.
4. Reconnect to a connected existing session in a non-preferred zone.
5. Start a new session in a non-preferred zone.

Other zone preference considerations

- If you configure a home zone for a user group (such as a security group), that group’s users (through direct or indirect membership) are associated with the specified zone. However, a user can be a member of multiple security groups, and therefore might have a different home zone configured through other group membership. In such cases, determination of that user’s home zone can be ambiguous.

If a user has a configured home zone that was not acquired through group membership, that zone is used for zone preference. Any zone associations acquired through group membership are ignored.

If the user has multiple different zone associations acquired solely through group membership, the broker chooses among the zones randomly. After the broker makes this choice, that zone is used for subsequent session launches, until the user’s group membership changes.

- The user location zone preference requires detection of Citrix Workspace app on the endpoint device by the Citrix Gateway through which that device is connecting. The Citrix must be configured to associate ranges of IP addresses with particular zones. Discovered zone identity must be passed through StoreFront to the Citrix Virtual Apps and Desktops service.

Although written for on-premises use of zones, the Zone Preference Internals blog post contains relevant technical details.

Permissions to manage zones

A Full Administrator can perform all supported zone management tasks. Moving items between zones does not require zone-related permissions (except zone read permission). However, you must have
edit permission for the items you are moving. For example, to move a machine catalog from one zone to another, you must have edit permission for that catalog.

If you use Citrix Provisioning: The current Citrix Provisioning console is not aware of zones, so Citrix recommends using Studio to create machine catalogs that you want to place in specific zones. Use the Studio wizard to create the catalog, specifying the zone. Then, use the Citrix Provisioning console to provision machines in that catalog.

Zone creation

When you create a resource location in Citrix Cloud and then add a Cloud Connector to that resource location, the Citrix Virtual Apps and Desktops service automatically creates and names a zone. You can optionally add a description later.

After you create more than one resource location (and the zones are created automatically), you can move resources from one zone to another.

Resource locations and zones are synchronized periodically, typically and approximately every five minutes. So, if you change a resource location’s name in Citrix Cloud, that change is propagated to the associated zone within five minutes.

Add or change a zone description

Although you cannot change a zone’s name, you can add or change its description in Studio.

1. Click Configuration > Zones in the navigation pane.
2. Select a zone in the middle pane and then click Edit Zone in the Actions pane.
3. Add or change the zone description.
4. Click OK or Apply.

Move resources from one zone to another zone

1. Click Configuration > Zones in the Studio navigation pane.
2. Select a zone in the middle pane, and then select one or more items.
3. Either drag the items to the destination zone or click Move Items in the Actions pane and then specify which zone to move them to. (Although you can select Cloud Connectors, you cannot actually move them to a different zone.)

A confirmation message lists the items you selected and asks if you are sure that you want to move all of them.
Remember: When a machine catalog uses a host connection to a hypervisor or cloud service, ensure that the catalog and the connection are in the same zone. Otherwise, performance can be affected. If you move one, move the other, too.

**Zone deletion**

You cannot delete a zone. However, you can delete a resource location (after removing its Cloud Connectors). Deleting the resource location automatically deletes the zone.

- If the zone does not contain any items (such as catalogs, connections, applications, or users), the zone is deleted during the next synchronization between zones and resource locations, which occurs every five minutes.
- If the zone contains items, the zone is automatically deleted after all items are removed.

**Add a home zone for a user**

Configuring a home zone for a user is also known as *adding a user to a zone*.

1. Click **Configuration > Zones** in the Studio navigation pane.
2. Select a zone in the middle pane and then click **Add Users to Zone** in the Actions pane.
3. In the **Add Users to Zone** dialog box, click **Add**, and then select the users and user groups to add to the zone. If you specify users who already have a home zone, a message offers two choices: **Yes** = add only those users you specified who do not have a home zone; **No** = return to the user selection dialog.
4. Click **OK**.

For users with a configured home zone, you can require that sessions launch only from their home zone:

1. Create or edit a Delivery Group.
2. On the **Users** page, select the **Sessions must launch in a user’s home zone, if configured** check box.

All sessions launched by a user in that Delivery Group must launch from machines in that user’s home zone. If a user in the Delivery Group does not have a configured home zone, this setting has no effect.

**Remove a home zone for a user**

This procedure is also known as removing a user from a zone.

1. Click **Configuration > Zones** in the Studio navigation pane.
2. Select a zone in the middle pane and then click **Remove Users from Zone** in the Actions pane.
3. In the **Add Users to Zone** dialog box, click **Remove**, and then select the users and groups to remove from the zone. This action removes the users only from the zone. Those users remain in the Delivery Groups to which they belong.
4. Confirm the removal when prompted.

**Manage home zones for applications**

Configuring a home zone for an application is also known as adding an application to a zone. By default, in a multi-zone environment, an application does not have a home zone.

An application’s home zone is specified in the application’s properties. You can configure application properties when you add the application to a group or later.

- When creating a **Delivery Group** or adding applications to existing groups, click **Properties** on the **Applications** page of the wizard.
- To change an application’s properties after the application is added, click **Applications** in the Studio navigation pane. Select an application and then click **Edit Application Properties** in the Actions pane.

On the **Zones** page of the application’s properties/settings:

- If you want the application to have a home zone:
  - Select the **Use the selected zone to decide** radio button and then select the zone.
  - If you want the application to launch only from the selected zone (and not from any other zone), select the check box under the zone selection.
- If you do not want the application to have a home zone:
  - Select the **Do not configure a home zone** radio button.
  - If you do not want the broker to consider any configured user zones when launching this application, select the check box under the radio button. In this case, neither application nor user home zones are used to determine where to launch this application.

**Other actions that include specifying zones**

If you have more than one zone, you can specify a zone when you add a host connection or create a catalog. Zones are listed alphabetically in selection lists. By default, the first alphabetical name is selected.

**Monitor**

March 21, 2019
Citrix Virtual Apps and Desktops service

Administrators and help-desk personnel can monitor Citrix Virtual Apps and Desktops service from Monitor, the monitoring and troubleshooting console. The Monitor tab displays a dashboard to monitor, troubleshoot, and perform support tasks for subscribers.

Note:
Monitor is available as the Director console to monitor and troubleshoot Citrix Virtual Apps and Desktops Current Release and LTSR deployments.

To access Monitor, sign in to Citrix Cloud. In the upper left menu, select My Services > Virtual Apps and Desktops. Click Monitor.

Monitor provides:

- Real-time data from the Broker Agent using a unified console integrated with Analytics and Performance Manager.
- Analytics includes performance management for health and capacity assurance, and historical trending to identify bottlenecks in your Citrix Virtual Apps or Desktops service environment.
- Historical data stored in the Monitor database to access the Configuration Logging database.
- Gain visibility into the end-user experience for virtual applications, desktops, and users for Citrix Virtual Apps or Desktops service.
- Monitor uses a troubleshooting dashboard that provides real-time and historical health monitoring of the Citrix Virtual Apps and Desktops service. This feature allows you to see failures in real time, providing a better idea of what the end users are experiencing.

Site Analytics

June 19, 2019

The Monitor dashboard provides a centralized location to monitor the health and usage of a Site.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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.

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Connection Failures</td>
<td>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. Connection failures includes failures caused by application limits being reached. For more information on application limits, see <a href="#">Applications</a>.</td>
</tr>
<tr>
<td>Failed Single session OS Machines or Failed Multi-session OS Machines</td>
<td>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 Multi-session OS machines, failures also include machines reaching maximum load.</td>
</tr>
<tr>
<td>Sessions Connected</td>
<td>Connected sessions across all Delivery Groups for the last 60 minutes.</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

Panel Description

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. For more information, see Diagnose user logon issues.

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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View a user's currently connected machine or</td>
<td>From the Activity Manager and User Details views, view the user's currently</td>
</tr>
<tr>
<td>session</td>
<td>connected machine or session and a list of all machines and sessions to which</td>
</tr>
<tr>
<td></td>
<td>this user has access. To access this list, click the session switcher icon</td>
</tr>
<tr>
<td></td>
<td>in the user title bar. For more information, see Restore sessions.</td>
</tr>
</tbody>
</table>
### Action Description

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the total number of connected sessions across all Delivery Groups</td>
<td>From the Dashboard, in the <strong>Sessions Connected</strong> 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.</td>
</tr>
<tr>
<td>End idle sessions</td>
<td>The Sessions Filters view displays data related to all active sessions. Filter the sessions based on Associated User, Delivery Group, Session State, and Idle Time greater than a threshold time period. From the filtered list, select sessions to log off or disconnect. For more information, see <a href="#">Troubleshoot applications</a>.</td>
</tr>
<tr>
<td>View data over a longer period of time</td>
<td>On the Trends view, select the <strong>Sessions</strong> 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 <strong>View historical trends</strong>.</td>
</tr>
</tbody>
</table>

### Note:

If the user device is running a legacy Virtual Delivery Agent (VDA), such as a VDA earlier than version 7, or a Linux VDA, Monitor cannot display complete information about the session. Instead, it displays a message that the information is not available.

### Desktop Assignment Rules limitation:

Citrix Studio allows assignment of multiple Desktop Assignment Rules (DAR) for different users or user groups to a single VDA in the Delivery Group. StoreFront displays the assigned desktop with the corresponding **DisplayName** as per the DAR for the logged in user. However, Monitor does not support DARs and displays the assigned desktop using the Delivery Group name regardless of the logged in user. As a result, you cannot map a specific desktop to a machine in Monitor.

You can map the assigned desktop displayed in StoreFront to the Delivery Group name displayed in Monitor using the following PowerShell command. Run the PowerShell command using Remote PowerShell SDK as described in the [blog](#).
Disable the visibility of running applications in the Activity Manager

By default, the Activity Manager displays a list of all running applications for a user’s session. This information can be viewed by all administrators that have access to the Activity Manager feature. 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 to list running applications. To do this, on the VDA, modify the registry key located at HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. By default, the key is set to 1. Change the value to 0, which means the information is not collected from the VDA and hence not displayed in the Activity Manager.

Warning:

Editing the registry 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.

Session transport protocol

View the transport protocol in use for the HDX connection type for the current session in the Session Details panel. This information is available for sessions launched on VDAs Version 7.13 or later.
• For **HDX** Connection type,
  – The Protocol is displayed as **UDP**, if EDT is used for the HDX connection.
  – The Protocol is displayed as **TCP**, if TCP is used for the HDX connection.
• For **RDP** Connection type, the Protocol is displayed as **n/a**.

When adaptive transport is configured, the session transport protocol dynamically switches between EDT (over UDP) and TCP, based on the network conditions. If the HDX session cannot be established
Citrix Virtual Apps and Desktops service

using EDT, it falls back to the TCP protocol.

For more information about adaptive transport configuration, see Adaptive Transport.

Export reports

You can export trends data to generate regular usage and capacity management reports. Export supports PDF, Excel, and CSV report formats. Reports in PDF and Excel formats contain trends represented as graphs and tables. CSV format reports contain tabular data that can be processed to generate views or can be archived.

To export a report:

1. Go to the Trends tab.
2. Set filter criteria and time period and click Apply. The trend graph and table are populated with data.
3. Click Export and enter name and format of the report.

Monitor generates the report based on the filter criteria you select. If you change the filter criteria, click Apply before you click Export.

Note:
Export of a large amount of data causes a significant increase in memory and CPU consumption on the Monitor server, the Delivery Controller, and the SQL servers. The supported number of concurrent export operations and the amount of data that can be exported is set to default limits to achieve optimal export performance.

Supported export limits

Exported PDF and Excel reports contain complete graphical charts for the selected filter criteria. However, tabular data in all report formats is truncated beyond the default limits on the number of rows or records in the table. The default number of records supported is defined based on the report format.

<table>
<thead>
<tr>
<th>Report format</th>
<th>Default number of records supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDF</td>
<td>500</td>
</tr>
<tr>
<td>Excel</td>
<td>100,000</td>
</tr>
<tr>
<td>CSV</td>
<td>100,000 (10,000,000 in Sessions tab)</td>
</tr>
</tbody>
</table>
Error Handling

Errors that you might encounter during an Export operation:

- **Director has timed out:** This error could occur due to network issues or high resource usage on the Director server or with the Monitor Service.

- **Monitor has timed out:** This error could occur due to network issues or high resource usage with the Monitor Service or on the SQL server.

- **Max concurrent Export or Preview operations ongoing:** Only one instance of Export or Preview can run at a specific time. If you get the **Max concurrent Export or Preview operations ongoing** error, try the next operation again later.

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 Monitor, use the Power Control options. These options are available for Single session OS machines, but might not be available for Multi-session OS machines.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restart</strong></td>
<td>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 Monitor as “failed to start,” and use this command to restart them.</td>
</tr>
<tr>
<td><strong>Force Restart</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Command</td>
<td>Function</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Shut Down</td>
<td>Performs an orderly (soft) shutdown of the VM; all running processes are halted individually.</td>
</tr>
<tr>
<td>Force Shutdown</td>
<td>Shuts down the VM without first performing any shut-down procedure. This command works in the same way as unplugging a physical server. It might not always shut down all running processes, and you risk losing data if you shut down a VM in this way.</td>
</tr>
<tr>
<td>Suspend</td>
<td>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.</td>
</tr>
<tr>
<td>Resume</td>
<td>Resumes a suspended VM and restores its original running state.</td>
</tr>
<tr>
<td>Start</td>
<td>Starts a VM when it is off (also called a cold start).</td>
</tr>
</tbody>
</table>

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
Application Analytics

The Applications tab displays application-based analytics in a single, consolidated view to help analyze and manage application performance efficiently. You can gain valuable insight into the health and usage information of all applications published on the Site. It shows metrics such as the probe results, number of instances per application, and faults and errors associated with the published applications. For more information, see the Application Analytics section in Troubleshooting Applications.

Alerts and notifications

June 19, 2019

Alerts are displayed in Monitor on the dashboard and other high level views with warning and critical alert symbols. Alerts update automatically every minute; you can also update alerts on demand.

A warning alert (amber triangle) indicates that the warning threshold of a condition has been reached or exceeded.

A critical alert (red circle) shows that the critical threshold of a condition has been reached or exceeded.

You can view more detailed information on alerts by selecting an alert from the sidebar, clicking the Go to Alerts link at the bottom of the sidebar or by selecting Alerts from the top of the Monitor page.
In the Alerts view, you can filter and export alerts. For example, Failed Multi-session OS machines for a specific Delivery Group over the last month, or all alerts for a specific user. For more information, see Export reports.

Citrix alerts

Citrix alerts are the ones that originate from Citrix components. You can configure Citrix alerts within Monitor in Alerts > Citrix Alerts Policy. As part of the configuration, you can set notifications to be sent by email to individuals and groups when alerts exceed the thresholds you have set up. For more information on setting up Citrix Alerts, see Create alerts policies.

Smart alert policies

A set of built-in alert policies with predefined threshold values are available for Delivery Groups and Multi-session OS VDAs scope. You can modify the threshold parameters of the built-in alert policies in Alerts > Citrix Alerts Policy. These policies are created when there is at least one alert target - a Delivery Group or a Multi-session OS VDA defined in your Site. Additionally, these built-in alerts are automatically added to a new delivery group or a Multi-session OS VDA.

Built-in alert policies are created only if no corresponding alert rules exist in the Monitor database. For the threshold values of the built-in alert policies, see the Alerts policies conditions section.
To create a new alerts policy, for example, to generate an alert when a specific set of session count criteria are met:

1. Go to **Alerts > Citrix Alerts Policy** and select, for example, Multi-session OS Policy.
2. Click **Create**.
3. Name and describe the policy, then set the conditions that have to be met for the alert to be triggered. For example, specify Warning and Critical counts for Peak Connected Sessions, Peak Disconnected Sessions, and Peak Concurrent Total Sessions. Warning values must not be greater than Critical values. For more information, see [Alerts policies conditions](#).
4. Set the Re-alert interval. If the conditions for the alert are still met, the alert is triggered again at
this time interval and, if set up in the alert policy, an email notification is generated. A dismissed alert does not generate an email notification at the re-alert interval.

5. Set the Scope. For example, set for a specific Delivery Group.

6. In Notification preferences, specify who should be notified by email when the alert is triggered. Email notifications are sent via SendGrid. Ensure that the email address 'donotreplynotifications@citrix.com' is white-listed in your email setup.

7. Click Save.

Creating a policy with 20 or more Delivery Groups defined in the Scope might take approximately 30 seconds to complete the configuration. A spinner is displayed during this time.

Creating more than 50 policies for up to 20 unique Delivery Groups (1000 Delivery Group targets in total) might result in an increase in response time (over 5 seconds).

Moving a machine containing active sessions from one Delivery Group to another might trigger erroneous Delivery Group alerts that are defined using machine parameters.

**Alerts policies conditions**

Find below the alert categories, recommended actions to mitigate the alert, and built-in policy conditions if defined. The built-in alert policies are defined for alert and realert intervals of 60 minutes.

**Peak Connected Sessions**

- Check Monitor Session Trends view for peak connected sessions.
- Check to ensure that there is enough capacity to accommodate the session load.
- Add new machines if needed

**Peak Disconnected Sessions**

- Check Monitor Session Trends view for peak disconnected sessions.
- Check to ensure that there is enough capacity to accommodate session load.
- Add new machines if needed.
- Log off disconnected sessions if needed

**Peak Concurrent Total Sessions**

- Check Monitor Session Trends view in Monitor for peak concurrent sessions.
- Check to ensure that there is enough capacity to accommodate session load.
- Add new machines if needed.
- Log off disconnected sessions if needed
CPU

Percentage of CPU usage indicates the overall CPU consumption on the VDA, including that of the processes. You can get more insight into the CPU utilization by individual processes from the Machine details page of the corresponding VDA.

- Go to Machine Details > View Historical Utilization > Top 10 Processes, identify the processes consuming CPU. Ensure that process monitoring policy is enabled to initiate collection of process level resource usage statistics.
- End the process if necessary.
- Ending the process causes unsaved data to be lost.
- If all is working as expected, add additional CPU resources in the future.

Note:
The policy setting, Enable resource monitoring is allowed by default for the monitoring of CPU and memory performance counters on machines with VDAs. If this policy setting is disabled, alerts with CPU and memory conditions are not triggered. For more information, see Monitoring policy settings.

Smart policy conditions:
- **Scope**: Delivery Group, Multi-session OS scope
- **Threshold values**: Warning - 80%, Critical - 90%

Memory

Percentage of Memory usage indicates the overall memory consumption on the VDA, including that of the processes. You can get more insight into the memory usage by individual processes from the Machine details page of the corresponding VDA.

- Go to Machine Details > View Historical Utilization > Top 10 Processes, identify the processes consuming memory. Ensure that process monitoring policy is enabled to initiate collection of process level resource usage statistics.
- End the process if necessary.
- Ending the process causes unsaved data to be lost.
- If all is working as expected, add additional memory in the future.

Note:
The policy setting, Enable resource monitoring, is allowed by default for the monitoring of CPU and memory performance counters on machines with VDAs. If this policy setting is
Citrix Virtual Apps and Desktops service

disabled, alerts with CPU and memory conditions are not triggered. For more information, see Monitoring policy settings.

Smart policy conditions:

- **Scope**: Delivery Group, Multi-session OS scope
- **Threshold values**: Warning - 80%, Critical - 90%

**Connection Failure Rate**

Percentage of connection failures over the last hour.

- Calculated based on the total failures to total connections attempted.
- Check Monitor Connection Failures Trends view for events logged from the Configuration log.
- Determine if applications or desktops are reachable.

**Connection Failure Count**

Number of connection failures over the last hour.

- Check Monitor Connection Failures Trends view for events logged from the Configuration log.
- Determine if applications or desktops are reachable.

**ICA RTT (Average)**

Average ICA round-trip time.

- Check Citrix ADM for a breakdown of the ICA RTT to determine the root cause. For more information, see Citrix ADM documentation.
- If Citrix ADM is not available, check the Monitor User Details view for the ICA RTT and Latency, and determine if it is a network problem or an issue with applications or desktops.

**ICA RTT (No. of Sessions)**

Number of sessions that exceed the threshold ICA round-trip time.

- Check Citrix ADM for the number of sessions with high ICA RTT. For more information, see Citrix ADM documentation.
- If Citrix ADM is not available, work with the network team to determine the root cause.

Smart policy conditions:

- **Scope**: Delivery Group, Multi-session OS scope
Citrix Virtual Apps and Desktops service

- **Threshold values**: Warning - 300 ms for 5 or more sessions, Critical - 400ms for 10 or more sessions

**ICA RTT (% of Sessions)**

Percentage of sessions that exceed the average ICA round-trip time.

- Check Citrix ADM for the number of sessions with high ICA RTT. For more information, see Citrix ADM documentation.
- If Citrix ADM is not available, work with the network team to determine the root cause.

**ICA RTT (User)**

ICA round-trip time that is applied to sessions launched by the specified user. The alert is triggered if ICA RTT is greater than the threshold in at least one session.

**Failed Machines (Single session OS)**

Number of failed Single session OS machines. Failures can occur for various reasons as shown in the Monitor Dashboard and Filters views.

- Run Citrix Scout diagnostics to determine the root cause. For more information, see Troubleshoot user issues.

**Smart policy conditions:**

- Scope: Delivery Group scope
- **Threshold values**: Warning - 1, Critical - 2

**Failed Machines (Multi-session OS)**

Number of failed Multi-session OS machines. Failures can occur for various reasons as shown in the Monitor Dashboard and Filters views.

- Run Citrix Scout diagnostics to determine the root cause.

**Smart policy conditions:**

- Scope: Delivery Group, Multi-session OS scope
- **Threshold values**: Warning - 1, Critical - 2
Citrix Virtual Apps and Desktops service

**Average Logon Duration**

Average logon duration for logons that occurred over the last hour.

- Check the Monitor Dashboard to get up-to-date metrics regarding the logon duration. A large number of users logging in during a short timeframe can increase the logon duration.
- Check the baseline and break down of the logons to narrow down the cause. For more information, see Diagnose user logon issues.

**Smart policy conditions:**
- **Scope:** Delivery Group, Multi-session OS scope
- **Threshold values:** Warning - 45 seconds, Critical - 60 seconds

**Logon Duration (User)**

Logon duration for logons for the specified user that occurred over the last hour.

**Load Evaluator Index**

Value of the Load Evaluator Index over the last 5 minutes.

- Check Monitor for Multi-session OS Machines that might have a peak load (Max load). View both Dashboard (failures) and Trends Load Evaluator Index report.

**Smart policy conditions:**
- **Scope:** Delivery Group, Multi-session OS scope
- **Threshold values:** Warning - 80%, Critical - 90%

**Hypervisor Alerts Monitoring**

Monitor displays alerts to monitor hypervisor health. Alerts from Citrix Hypervisor and VMware vSphere help monitor hypervisor parameters and states. The connection status to the hypervisor is also monitored to provide an alert if the cluster or pool of hosts is rebooted or unavailable.

To receive hypervisor alerts, ensure that a hosting connection is created in the Manage tab. For more information, see Connections and resources. Only these connections are monitored for hypervisor alerts. The following table describes the various parameters and states of Hypervisor alerts.
## Supported Hypervisors

<table>
<thead>
<tr>
<th>Alert</th>
<th>Triggered by</th>
<th>Condition</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU usage</td>
<td>Citrix Hypervisor, VMware vSphere</td>
<td>Hypervisor</td>
<td>CPU usage alert threshold is reached or exceeded</td>
</tr>
<tr>
<td>Memory usage</td>
<td>Citrix Hypervisor, VMware vSphere</td>
<td>Hypervisor</td>
<td>Memory usage alert threshold is reached or exceeded</td>
</tr>
<tr>
<td>Network usage</td>
<td>Citrix Hypervisor, VMware vSphere</td>
<td>Hypervisor</td>
<td>Network usage alert threshold is reached or exceeded</td>
</tr>
<tr>
<td>Disk usage</td>
<td>VMware vSphere</td>
<td>Hypervisor</td>
<td>Disk usage alert threshold is reached or exceeded</td>
</tr>
<tr>
<td>Host connection or power state</td>
<td>VMware vSphere</td>
<td>Hypervisor</td>
<td>Hypervisor Host has been rebooted or is unavailable</td>
</tr>
<tr>
<td>Hypervisor connection unavailable</td>
<td>Citrix Hypervisor, VMware vSphere</td>
<td>Delivery Controller</td>
<td>Connection to the hypervisor (pool or cluster) is lost or powered down or rebooted. This alert is generated every hour as long as the connection is unavailable.</td>
</tr>
</tbody>
</table>
Note:
For more information about configuring alerts, see Citrix XenCenter Alerts or VMware vCenter Alerts.

Email notification preference can be configured under Citrix Alerts Policy > Site Policy > Hypervisor Health. The threshold conditions for Hypervisor alert policies can be configured, edited, disabled, or deleted from the hypervisor only and not from Monitor. However, modifying email preferences and dismissing an alert can be done in Monitor.

Important:

- Alerts triggered by the Hypervisor are fetched and displayed in Monitor. However, changes in the life cycle/state of the Hypervisor alerts are not reflected in Monitor.
- Alerts that are healthy or dismissed or disabled in the Hypervisor console will continue to appear in Monitor and have to be dismissed explicitly.
- Alerts that are dismissed in Monitor are not dismissed automatically in the Hypervisor console.

A new Alert category called Hypervisor Health has been added to enable filtering only the hypervisor alerts. These alerts are displayed once the thresholds are reached or exceeded. Hypervisor alerts can be:

- Critical—critical threshold of the hypervisor alarm policy reached or exceeded
- Warning—warning threshold of the hypervisor alarm policy reached or exceeded
- Dismissed—alert no longer displayed as an active alert

**Filter data to troubleshoot failures**

July 2, 2019

When you click numbers on the Dashboard or select a predefined filter from the Filters menu, the Filters view opens to display 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, sessions, and application instances across all Delivery Groups.

1. Select a view:
   - **Machines.** Select Single session OS Machines or Multi-session OS Machines. These views show the number of configured machines. The Multi-session 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 Sessions view. Use the idle time measurements to identify sessions that are idle beyond a threshold time period.
   - **Connections.** Filter connections by different time periods, including last 60 minutes, last 24 hours, or last 7 days.
   - **Application Instances.** This view displays the properties of all application instances on VDAs of Multi-session and Single session OS. The session idle time measurements are available for Application instances on VDAs of Multi-session OS.

2. For **Filter 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.

6. To open the filter later, from the **Filters** menu, select the filter type (Machines, Sessions, Connections, or Application Instances), and then select the saved filter.

7. Click **Export** to export the data to CSV format files. Data of up to 100,000 records can be exported.

8. If needed, for **Machines** or **Connections** views, use power controls for all the machines you select in the filtered list. For the Sessions view, use the session controls or option to send messages.

9. In the **Machines** and **Connections** views, click the **Failure Reason** of a failed machine or connection to get a detailed description of the failure and actions recommended to troubleshoot the failure. The failure reasons and the recommended actions for Machine and Connection failures are available in the Citrix Director Failure Reasons Troubleshooting Guide.

10. In the **Machines** view, click on a machine name link to go to the corresponding **Machine Details** page. This page displays the details of the machine, provides power controls, displays the CPU, memory, disk monitoring, and GPU monitoring graphs. Also, click **View Historical Utilization** to see the resource utilization trends for the machine. For more information, see Troubleshoot machines.
11. In the **Application Instances** view, sort or filter based on **Idle Time** greater than a threshold time period. Select the idle application instances to end. Log off or Disconnect of an application instance ends all active application instances in the same session. For more information, see **Troubleshoot applications**. The Application Instances filter page and idle time measurements in the Sessions filter pages are available if VDAs are version 7.13 or later.

**Note:**

Citrix Studio allows assignment of multiple Desktop Assignment Rules (DAR) for different users or user groups to a single VDA in the Delivery Group. StoreFront displays the assigned desktop with the corresponding Display Name as per the DAR for the logged in user. However, Monitor does not support DARs and displays the assigned desktop using the Delivery Group name regardless of the logged in user. As a result, you cannot map a specific desktop to a machine in Monitor. To map the assigned desktop displayed in StoreFront to the Delivery Group name displayed in Monitor, use the following PowerShell command. Run the PowerShell command using Remote PowerShell SDK as described in the [blog](#).

```powershell
Get-BrokerDesktopGroup | Where-Object {
    $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
        $_.PublishedName -eq "<Name on StoreFront>"
    }).DesktopGroupUid
} | Select-Object -Property Name, Uid
```

---

**Monitor historical trends across a Site**

**August 27, 2019**

The Trends view accesses historical trend information for sessions, connection failures, application failures, application probe results, machine failures, logon performance, load evaluation, capacity management, machine usage and resource utilization for the Site. To locate this information, click the **Trends** menu.

The zoom-in drill down feature lets you navigate through trend charts by zooming in on a time period (clicking 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.

**Note:**

- Sessions, failures, and logon performance trend information are available as graphs and
tables when the time period is set to Last month (Ending now) or shorter. When the time period is chosen as Last month with a custom ending date or as Last year, the trend information is available as graphs but not as tables.

- Citrix Virtual Apps and Desktops service supports historical data retention only for 90 days. Hence, one-year trends and reports in Monitor show the last 90 days of data.

Available trends

**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.

The Session Auto Reconnect column displays the number of auto reconnects in a session. Auto reconnect is enabled when the Session Reliability or the Auto Client Reconnect policies are in effect. When there is a network interruption on the endpoint, the following policies come into effect:

- Session reliability comes into effect (by default for 3 minutes) where the Citrix Receiver or Citrix Workspace app tries to connect to the VDA.
- Auto Client reconnect comes into effect between 3 and 5 minutes where the client tries to connect to the VDA.

Both these reconnects are captured and displayed to the user. This information can take a maximum time of 5 minutes to appear on the Director UI after the reconnect occurs.

The auto reconnect information helps you view and troubleshoot network connections having interruptions, and to analyze networks having a seamless experience. You can view the number of reconnects for a specific Delivery Group or time period selected in the Filters. A drilldown provides additional information like Session Reliability or Auto Client Reconnect, time stamps, Endpoint IP, and Endpoint Name of the machine where Workspace app is installed. By default, logs are sorted by the event time stamps in descending order. This feature is available for Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Receiver for Windows, and Citrix Receiver for Mac. This feature requires VDAs 1906 or later. For more information about session reconnections, see Sessions. For more information about policies, see Auto client reconnect policy settings and Session reliability policy settings.

Sometimes, the auto reconnect data might not appear in Monitor for the following reasons:

- Workspace app is not sending auto reconnect data to VDA.
- VDA is not sending data to monitor service.

**Note:**

Sometimes, the client IP address might not be obtained correctly if certain NSG policies are set.
View trends for connection failures: From the Failures tab, select the connection, 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 Single session OS Machine Failures tab or Multi-session 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 and VM start time. This data is specifically for user logons and does not include users trying to reconnect from disconnected sessions.

The table below the graph shows Logon Duration by User Session. You can choose the columns to display and sort the report by any of the columns. For more information, see Diagnose user logon issues.

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 Multi-session OS machines. The filter options for this graph include the Delivery Group or Multi-session OS machine in a Delivery Group, Multi-session OS machine (available only if Multi-session OS machine in a Delivery Group was selected), and range. The Load Evaluator Index is displayed as percentages of Total CPU, Memory, Disk or Sessions and is shown in comparison with the number of connected users in the last interval.

View hosted applications usage: From the Capacity Management tab, select 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. You can see the predicted peak concurrent application instances values chosen future time period with Application instance prediction. For more information, see the Application instance prediction section.

View single and multi-session OS usage: The Trends view shows the usage of Single session OS by Site and by Delivery Group. When you select Site, usage is shown per Delivery Group. When you select Delivery Group, usage is shown per User.

The Trends view also shows the usage of Multi-session OS by Site, by Delivery Group, and by Machine. When you select Site, usage is shown per Delivery Group. When you select Delivery Group, usage is shown per Machine and per User. When Machine is selected usage is shown per User.

View virtual machine usage: From the Machine Usage tab, select Single session OS Machines or Multi-session OS Machines to obtain a real-time view of your VM usage. The page displays the number of Autoscale enabled Multi-session and Single session OS machines that are powered on for a selected De-
livery Group and time period. Also available is the estimated savings achieved by enabling Autoscale in the selected Delivery Group, this percentage is calculated using the per machine costs.

The usage trends of Autoscale enabled machines indicate the actual usage of the machines, enabling you to quickly assess your Site's capacity needs.

- Single session OS availability - displays the current state of Single session OS machines (VDIs) by availability for the entire Site or a specific Delivery Group.
- Multi-session OS availability - displays the current state of Multi-session OS machines by availability for the entire Site or a specific Delivery Group.

**Note:**
The grid below the chart displays the Delivery Group based machine usage data in real-time. The data includes machine availability of all machines independent of Autoscale enablement. The number of machines displayed in the Available Counter column in the grid includes machines in maintenance mode.

The monitoring data consolidation depends on the time period you select.

- Monitoring data for the one day and one week time periods is consolidated per hour.
- Monitoring data for the one month time period is consolidated per day.

The machine status is read at the time of consolidation and any changes during the period in between is not considered. For the consolidation period, refer to the Monitor API documentation.

For more information on monitoring autoscale enabled machines see the Autoscale article.

**View resource utilization:** From the Resource Utilization tab, select Single session OS Machines or Multi-session OS Machines to obtain insight into historical trends data for CPU and memory usage, and IOPS and disk latency for each VDI machine for better capacity planning. This feature requires VDAs version 7.11 or later.

Graphs show data for average CPU, average memory, average IOPS, disk latency, and peak concurrent sessions. You can drill down to the machine, and view data and charts for the top 10 processes consuming CPU. Filter by Delivery Group and Time period. CPU, memory usage, and peak concurrent sessions graphs are available for the last 2 hours, 24 hours, 7 days, month, and year. The average IOPS and disk latency graphs are available for the last 24 hours, month, and year.

**Note:**
- The Monitoring policy setting, Enable Process Monitoring, must be set to "Allowed” to collect and display data in the Top 10 Processes table on the Historic Machine Utilization page. The policy is set to "Prohibited" by default. All resource utilization data is collected by default. This can be disabled using the Enable Resource Monitoring policy setting. The table below the graphs shows the resource utilization data per machine.
- Average IOPS shows the daily averages. Peak IOPS is calculated as the highest of the IOPS
Citrix Virtual Apps and Desktops service

Averages for the selected time range. (An IOPS average is the hourly average of IOPS collected during the hour on the VDA).

**View application failures:** The Application Failures tab displays failures associated with the published applications on the VDAs.

This feature requires VDAs version **7.15** or later. Single session OS VDAs running Windows Vista and later, and Multi-session OS VDAs running Windows Server 2008 and later are supported. For more information, see **Historical application failure monitoring**.

By default, only application faults from Multi-session OS VDAs are displayed. You can set the monitoring of application failures by using Monitoring policies. For more information, see **Monitoring policy settings**.

**View application probe results:** The Application Probe Results tab displays the results of probe for applications that have been configured for probing in the Configuration page. Here, the stage of launch during which the application launch failure occurred is recorded.

This feature requires VDAs version **7.18** or later. For more information see **Application probing**.

**Create customized reports:** The Custom Reports tab provides a user interface for generating Custom Reports containing real-time and historical data from the Monitoring database in tabular format.

From the list of previously saved Custom Report queries, you can click **Run and download** to export the report in CSV format, click **Copy OData** to copy and share the corresponding OData query, or click **Edit** to edit the query.

You can create a new Custom Report query based on machines, connections, sessions, or application instances. Specify filter conditions based on fields such as machine, Delivery Group, or time period. Specify additional columns required in your Custom Report. Preview displays a sample of the report data. Saving the Custom Report query adds it to the list of saved queries.

You can create a new Custom Report query based on a copied OData query. To do this, select the OData Query option and paste the copied OData query. You can save the resultant query for execution later.

**Note:**

The column names in Preview and Export report generated using OData queries are not localized, but appear in English.

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.
- Delivery Groups deleted in Citrix Studio are available for selection in the Trends filters until

© 1999-2019 Citrix Systems, Inc. All rights reserved.
data related to them are groomed out. Selecting a deleted Delivery Group displays graphs for available data until retention. However, the tables don’t show data.

- Moving a machine containing active sessions from one Delivery Group to another causes the Resource Utilization and Load Evaluator Index tables of the new Delivery Group to display metrics consolidated from the old and new Delivery Groups.

**Application instance prediction**

Predictive analytics gives you the ability to predict future resource usage. This feature is especially useful for administrators to organize required resources and licenses on each resource.

The first predictive analysis feature, Application instance prediction predicts the number of hosted application instances likely to be launched per Site or Delivery Group over time.

Application instance prediction is available in the Trends > Capacity Management tab that displays the hosted application usage for the chosen time period. The historical graph contains the peak concurrent application instances values plotted for the chosen period.

To get the predicted graph, select the Predict check box. A dotted line prediction graph is displayed as an extension of the historical graph. The predicted peak concurrent application instances values are plotted with the timeline extended into the future for the chosen time period.

You can predict the application instances for time periods of the next 7 days, one month, or one year. Custom ending dates are not supported.

Prediction is done using machine learning algorithms that are based on data models created with existing historical data. The predictions are therefore as accurate as the quality of the existing data.

The accuracy of prediction is indicated by the tolerance level that is displayed as a tool tip over the predicted graph. It indicates the amount of possible variation of the actual values from the predicted values.
Citrix Virtual Apps and Desktops service

The tolerance level can be high if either the available data does not follow a regular pattern or is missing for certain periods or is insufficient.

Prediction for a year captures the monthly and quarterly patterns coupled with the overall trend for the year. Similarly, monthly prediction captures the daily and weekly patterns along with weekly trends such as reduced activity over weekends.

Sufficient historical data must be available for prediction as follows:

- 14 days data for 7 days' prediction
- 35 days data for one month's prediction
- 84 days data for one year's prediction

Note
You can export only the historical graph, but not the predicted graph.
For a short demonstration of the Application instance prediction feature, see the video.

Monitor Autoscale-managed machines

July 10, 2019

Autoscale is a power management feature that enables proactive power management of all registered Multi-session and Single session OS machines in a Delivery Group. You can configure Autoscale for a selected Delivery Group from the Manage tab. For more information, see Autoscale. You can monitor the key metrics of Autoscale enabled machines from the Monitor tab.

Machine Usage

The Monitor > Trends > Machine Usage page displays the total number of Autoscale enabled Multi-session and Single session OS machines that are powered on for a selected Delivery Group and time period. This metric indicates the actual usage of machines in the Delivery Group. From the Single session OS Machines or the Multi-session OS Machines tab, select the Delivery group and the time period.
The chart plots the following metrics:

- **Machines On** - the number of Autoscale enabled machines that are powered on
- **Machines Registered** - the number of registered Multi-session or Single session OS machines
- **Machines under Maintenance** - the number of Multi-session or Single session OS machines with maintenance mode switched on

**Estimated Savings**

The Monitor > Trends > Machine Usage page also displays the estimated cost savings achieved by enabling Autoscale in the selected Delivery Group.
Estimated Savings is calculated as the percentage of savings per machine per hour (in US $) as configured in Manage > Edit Delivery Group > Autoscale. For more information about configuring the savings per machine, see Autoscale.

When you select all Delivery groups, the average value of Estimated Savings across all the Delivery Groups is displayed.

The estimated savings help administrators consolidate the existing infrastructure and plan the capacity to achieve maximum savings and utilization.

**Alert notifications for machines and sessions**

The Monitor Dashboard displays alert notifications that can be further drilled down. Alert details are displayed on the Monitor > Alerts page.

- To create an alert policy in a Delivery Group, go to Monitor > Alerts > Citrix Alerts Policy > Delivery Group Policy.
- Here, you can set the following Warning and Critical thresholds:
  - Failed Machines (Single session OS) and Failed Machines (Multi-session OS),
  - Peak Connected Sessions, Peak Disconnected Sessions and Peak Concurrent Total Sessions in the Delivery Group.
- Alerts are generated when the corresponding metric in the Delivery Group reaches the threshold.

For more details regarding the alert policy conditions and creation of new alert policies, see Alerts and notifications.
Machine status

- **Monitor > Filters > Machines** displays the power state of all machines in a tabular format. You can filter by a specific Delivery Group.
- **Monitor > Filters > Sessions** displays filter by the Machine name to see the associated sessions and their real-time status.
- In **Monitor > Trends > Sessions**, select your Delivery Group and time period to see the trend of the sessions and their associated metrics.

For more information, see [Filter data to troubleshoot failures](#).

Load Evaluation trends

The **Monitor > Trends > Load Evaluator Index** page displays a graph with detailed information about the load that is distributed among the Multi-session OS machines. The filter options for this graph include the Delivery Group or Multi-session OS machine in a Delivery Group, Multi-session OS machine (available only if Multi-session OS machine in a Delivery Group was selected), and range. The Load Evaluator Index is displayed as percentages of Total CPU, Memory, Disk, or Sessions and is shown in comparison with the number of connected users in the last interval.

Troubleshoot deployments

March 15, 2019

As a help desk administrator, you can search for the user reporting an issue and display details of sessions or applications associated with that user. Similarly, you can search for machines or endpoints where issues are reported. Issues can be quickly resolved by monitoring the relevant metrics and performing suitable actions. Available actions include ending an unresponsive application or process, shadowing operations on the user’s machine, logging off an unresponsive session, restarting the machine, putting a machine into maintenance mode or resetting the user profile.

Troubleshoot applications

July 2, 2019
Application Analytics

The **Applications** view displays application-based analytics in a single, consolidated view to help analyze and manage application performance efficiently. You can gain valuable insight into the health and usage information of all applications published on the Site. The default view helps identify the top running applications. This feature requires VDAs Version 7.15 or later.

The **Probe Result** column displays the result of application probing run in the last 24 hours. Click the probe result link to see more details in the **Trends > Application Probe Results** page. For more details on how to configure application probes, see Application Probing.

The **Instances** column displays usage of the applications. It indicates the number of application instances currently running (both connected and disconnected instances). To troubleshoot further, click the **Instances** field to see the corresponding **Application Instances** filters page. Here, you can select application instances to log off or disconnect.

**Note:**

For custom scope administrators, Monitor does not display application instances created under Application Groups. To view all application instances, you must be a full administrator. For more information, see Knowledge Center article CTX256001.

Monitor the health of published applications in your Site with the **Application Faults** and the **Application Errors** columns. These columns display the aggregated number of faults and errors that have occurred while launching the corresponding application in the last one hour. Click the **Application Faults** or **Application Errors** field to see failure details on the **Trends > Application Failures** page corresponding to the selected application.

The application failure policy settings govern the availability and display of faults and errors. For more information about the policies and how to modify them, see Policies for application failure monitoring.
Real-time application monitoring

You can troubleshoot applications and sessions by using the idle time metric to identify instances that are idle beyond a specific time limit.

Typical use cases for application-based troubleshooting are in the healthcare sector, where employees share application licenses. There, you must end idle sessions and application instances to purge the Citrix Virtual Apps and Desktops environment, to reconfigure poorly performing servers, or to maintain and upgrade applications.

The Application Instances filter page lists all application instances on VDAs of Multi-session and Single session OS. The associated idle time measurements are displayed for application instances on VDAs of Multi-session OS that have been idle for at least 10 minutes.

Note:

The Application Instances metrics are available on Sites of all license editions.

Use this information to identify the application instances that are idle beyond a specific time period and log off or disconnect them as appropriate. To do this, select Filters > Application Instances and select a pre-saved filter or choose All Application Instances and create your own filter.

An example of a filter would be as follows. As Filter by criteria, choose Published Name (of the application) and Idle Time. Then, set Idle Time to greater than or equal to a specific time limit and save the filter for reuse. From the filtered list, select the application instances. Select option to send messages or from the Session Control drop-down, choose Logoff or Disconnect to end the instances.
Note:
Logging off or disconnecting an application instance logs off or disconnects the current session, thereby ending all application instances that belong to the same session.

You can identify idle sessions from the Sessions filter page using the session state and the session idle time metric. Sort by the Idle Time column or define a filter to identify sessions that are idle beyond a specific time limit. Idle time is listed for sessions on VDAs of Multi-session OS that have been idle for at least 10 minutes.

The Idle time is displayed as N/A when the session or application instance

- has not been idle for more than 10 minutes,
- is launched on a VDA of Single session OS, or
- is launched on a VDA running Version 7.12 or earlier.

Historical application failure monitoring

The Trends -> Application Failures tab displays failures associated with the published applications on the VDAs.

Application failure trends are available for the last 2 hours, 24 hours, 7 days, and month for Premium and Advanced licensed Sites. They are available for the last 2 hours, 24 hours, and 7 days for other license types. The application failures that are logged to the Event Viewer with source “Application Errors” are monitored. Click Export to generate reports in CSV, Excel, or PDF formats
The failures are displayed as **Application Faults** or **Application Errors** based on their severity. The Application Faults tab displays failures associated with loss of functionality or data. Application Errors indicate problems that are not immediately relevant; they signify conditions that might cause future problems.

You can filter the failures based on **Published Application Name**, **Process Name** or **Delivery Group**, and **Time Period**. The table displays the fault or error code and a brief description of the failure. The detailed failure description is displayed as a tooltip.

**Note:**

The Published Application name is displayed as “Unknown” when the corresponding application name cannot be derived. This typically occurs when a launched application fails in a desktop session or when it fails due to an unhandled exception caused by a dependent executable.

By default, only faults of applications hosted on Multi-session OS VDAs are monitored. You can modify the monitoring settings through the Monitoring Group Policies: Enable monitoring of application failures, Enable monitoring of application failures on Single session OS VDAs, and List of applications excluded from failure monitoring. For more information, see Policies for application failure monitoring in Monitoring policy settings.

The **Trends > Application Probe Results** page displays the results of application probing executed in the Site for the last 24 hours and 7 days. For more details on how to configure application probes, see Application Probing.

**Application probing**

June 13, 2019
Citrix Virtual Apps and Desktops service

Application probing automates the process of checking the health of Citrix Virtual Apps that are published in a Site. The results of application probing are available in the Monitor tab of Citrix Virtual Apps and Desktops service.

Ensure that the endpoint machines running probe agents are Windows machines with Citrix Receiver for Windows Version 4.8 or later, or Citrix Workspace app for Windows (formerly Citrix Receiver for Windows) Version 1808 or later. Workspace app for Unified Windows Platform (UWP) is not supported.

User accounts/permissions required to run Application Probing are as follows:

- A unique Workspace user to probe on each endpoint machine. The Workspace user is not required to be an administrator; the probes can run in a non-admin context.
- User accounts with Windows administrator permissions to install and configure the Citrix Probe Agent on the endpoint machines
- A full administrator user account with the following permissions. Reusing existing user accounts for application probing might log off the users’ active sessions.
  - Delivery Group permissions:
    - Read-only
  - Director permissions:
    - Create\Edit\Remove Probe Configurations
    - View Configurations page
    - View Trends page

Configure Application Probing

Configure your application probes to run during off-peak hours across multiple geographies. The comprehensive probe results can help to troubleshoot issues related to the applications, hosting machine or connection before the users experience them.

Step 1: Install and configure the Citrix Probe Agent

The Citrix Probe Agent is a Windows executable that simulates the actual application launch by the user through Citrix Workspace. It tests application launches as configured in Monitor and reports back the results to Monitor.

1. Identify endpoint machines from where you want to run application probing.


3. Start the agent and configure your Citrix Workspace credentials. Configure a unique Workspace user on each endpoint machine. The credentials are encrypted and stored securely.
Note:
To access the Site to be probed from outside the network, type the login URL for Citrix Gateway in the **Workspace URL** field. Citrix Gateway automatically routes the request to the corresponding Site Workspace URL.

4. In the **Configure To Display Probe Result** tab, enter credentials to access the Citrix Virtual Apps and Desktops service.

Note:
You can find the Customer Name, Client ID, and Secret Key from the API Access page in the Citrix Cloud console.

Step 2: Configure Application probing in the Monitor tab

1. In the Citrix Virtual Apps and Desktops service, go to **Configuration > Application Probe Configuration**.

2. Create a probe and choose:
   - the applications to be probed,
   - the endpoint machines on which the probe must run,
   - the email addresses to which the failure probe results are sent,
• the time of the day at which the probe must run (as per the local time zone of the endpoint machine).

After configuration in the Monitor tab, the agent takes 10 minutes before it is ready to start probing. Then, it runs configured probes starting the next hour.

**Step 3: Probe execution**

The agent executes application probing as per the probe configuration it fetches from Monitor every hour. It launches selected applications serially using Workspace. The agent reports the results back to Monitor via the Monitor database. Failures are reported in five specific stages:

- **Workspace Reachability** - configured Workspace URL is not reachable.
- **Workspace Authentication** - configured Workspace credentials are invalid.
- **Workspace Enumeration** - Workspace Enumerate applications list does not contain the application to be probed.
- **ICA download** - the ICA file is not available.
- **Application launch** – the application cannot be launched.

**Step 4: View probe results**

You can view the latest probe results in the Citrix Virtual Apps and Desktops service > Applications page.
To troubleshoot further, click the probe result link to see more details on the Trends > Application Probe Results page.

The consolidated probe results data is available for the last 24 hours or last 7 days time periods on this page. You can see the stage in which the probe failed. You can filter the table for a specific application, probe failure stage, or endpoint machine.

**Desktop probing**

**July 15, 2019**

Desktop probing automates the process of checking the health of Citrix Virtual Desktops that are published in a Site. The results of desktop probing are available in Monitor.

In Monitor’s Configuration page, configure the desktops to be probed, the endpoint machines to run...
the probe on, and the probe time. The agent tests the launch of selected desktops using Workspace and reports the results back to Monitor. The probe results are displayed on the Monitor UI – the last 24-hours’ data on the Applications page and historical probe data on the Trends > Probe Results > Desktop Probe Results page. Here, you can see the stage when the probe failure occurred - Workspace Reachability, Workspace Authentication, Workspace Enumeration, ICA download, or Desktop launch. The failure report is sent to the configured email addresses. You can schedule your desktop probes to run during off-peak hours across multiple geographies. The comprehensive results can help to proactively troubleshoot issues related to provisioned desktops, hosting machines or connections before the users experience them. Desktop probing is available for Premium licensed Sites. This feature requires Probe Agent 1903 or later.

Requirements:

- Endpoint machines running probe agents are Windows machines with Citrix Receiver for Windows Version 4.8 or later, or Citrix Workspace app for Windows (formerly Citrix Receiver for Windows) Version 1906 or later. Workspace app for Unified Windows Platform (UWP) is not supported.
- Monitor and Workspace support the default form-based authentication.

User accounts or permissions required to run Desktop probing:

- A unique Workspace user to probe on each endpoint machine. The Workspace user need not be an administrator; the probes can run in a non-admin context.
- User accounts with Windows administrator permissions to install and configure the Citrix Probe Agent on the endpoint machines.
- A full administrator user account or a custom role with the following permissions. Reusing normal user accounts for desktop probing might log off the users’ active sessions.
  - Delivery Group permissions:
    - Read-only
  - Monitor permissions:
    - Create, Edit, Remove Alert Email Server Configuration - if the email server is not already configured
    - Create, Edit, Remove Probe Configurations
    - View Configurations page
    - View Trends page

Configure desktop probing

You can schedule your desktop probes to run during off-peak hours across multiple geographies. The comprehensive probe results can help to troubleshoot issues related to the desktops, hosting machine or connection before the users experience them.
Step 1: Install and configure the Citrix Probe Agent

The Citrix Probe Agent is a Windows executable that simulates the actual desktop launch by the user through Workspace. It tests desktop launches as configured in Monitor and reports back the results to Monitor.

1. Identify endpoint machines from where you want to run desktop probing.
3. Start the agent and configure your Workspace Receiver for Web credentials. Configure a unique Workspace user on each endpoint machine. The credentials are encrypted and stored securely.
   
   Note:
   
   To access the Site to be probed from outside the network, type the Citrix Gateway login page URL on the Workspace URL field. Citrix Gateway automatically routes the request to the corresponding Site Workspace URL. This feature is available for Citrix Gateway version 12.1 or later.

4. On the Configure To Display Probe Result tab, enter your Monitor credentials.

Step 2: Configure desktop probing in Monitor

1. Go to Configuration > Desktop Probe Configuration.
2. To create a probe, enter the details and click **Save**.

![Configuration](image)

**Note:**

Configure your email server in **Alerts > Email Server Configuration**.

After desktop probing configuration is complete, the agent takes 10 minutes before it is ready to start probing. Then, it runs configured probes starting the next hour.

**Step 3: Probe execution**

The agent executes desktop probing as per the probe configuration it fetches from Monitor periodically. It launches selected desktops serially using Workspace. The agent reports the results back to Monitor via the Monitor database. Failures are reported in five specific stages:

- **Workspace Reachability** - configured Workspace URL is not reachable.
- **Workspace Authentication** - configured Workspace credentials are invalid.
- **Workspace Enumeration** - Workspace Enumerate desktops list does not contain the desktop to be probed.
- **ICA download** - the ICA file is not available.
- **Desktop launch** – the desktop cannot be launched.

**Step 4: View probe results**

You can view the latest probe results on the **Desktops** page.
To troubleshoot further, click the probe result link to see more details on the **Trends > Probe Results > Desktop Probe Results** page.

![Desktop Probe Results page](image)

The consolidated probe results data is available for the last 24 hours or last 7 days' time periods on this page. You can see the stage in which the probe failed. You can filter the table for a specific desktop, probe failure stage, or endpoint machine.

**Troubleshoot machines**

July 2, 2019

**Note:**

**Citrix Health Assistant** is a tool to troubleshoot configuration issues in unregistered VDAs. The tool automates a number of health checks to identify possible root causes for VDA registration failures and issues in session launch and time zone redirection configuration. The Knowledge Center article, **Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch** con-
Citrix Virtual Apps and Desktops service

The **Citrix Health Assistant** tool download and usage instructions.

The **Filters > Machines** view in the Monitor tab displays the machines configured in the Site. The Multi-session OS Machines tab includes the load evaluator index, which indicates the distribution of performance counters and tooltips of the session count if you hover over the link.

Click the **Failure Reason** column of a failed machine to get a detailed description of the failure and actions recommended to troubleshoot the failure. The failure reasons and the recommended actions for machine and connection failures are available in the **Citrix Director Failure Reasons Troubleshooting Guide**.

Click the machine name link to go to the **Machine Details** page.

The Machine Details page lists the machine details, infrastructure details, and details of the hotfixes applied on the machine.

**Machine-based real-time resource utilization**

The **Machine Utilization** panel displays graphs showing real-time utilization of CPU and memory. In addition, disk and GPU monitoring graphs are available for Sites with VDA versions 7.14 or later.

Disk monitoring graphs, average IOPS, and disk latency are important performance measurements that help you monitor and troubleshoot issues related to VDA disks. The Average IOPS graph displays the average number of reads and writes to a disk. Select **Disk Latency** to see a graph of the delay between a request for data and its return from the disk, measured in milliseconds.

Select **GPU Utilization** to see percentage utilization of the GPU, the GPU memory, and of the Encoder and the Decoder to troubleshoot GPU-related issues on Multi-session or Single session OS VDAs. The GPU Utilization graphs are available only for VDAs running 64-bit Windows with NVIDIA Tesla M60 GPUs, and running Display Driver version 369.17 or later.
Citrix Virtual Apps and Desktops service

The VDAs must have HDX 3D Pro enabled to provide GPU acceleration. For more information, see GPU acceleration for Windows Single session OS and GPU acceleration for Windows Multi-session OS. When a VDA accesses more than one GPU, the utilization graph displays the average of the GPU metrics collected from the individual GPUs. The GPU metrics are collected for the entire VDA and not for individual processes.

**Machine-based historical resource utilization**

In the **Machine Utilization** panel, click **View Historical Utilization** to view the historical usage of resources on the selected machine.

The utilization graphs include critical performance counters of CPU, memory, peak concurrent sessions, average IOPS, and disk latency.

**Note:**

The Monitoring policy setting, **Enable Process Monitoring**, must be set to Allowed to collect, and display data in the Top 10 Processes table on the Historic Machine Utilization page. The collection is prohibited by default.

The CPU and memory utilization, average IOPS, and disk latency data is collected by default. You can disable the collection by using the **Enable Resource Monitoring** policy setting.
1. From the **Machine Utilization** panel in the **Machine Details** view, select **View Historical Utilization**.

2. In the **Historical Machine Utilization** page, set **Time Period** to view usage for the last 2 hours, 24 hours, 7 days, month, or year.

   **Note:**
   Average IOPS and disk latency usage data are available only for the last 24 hours, month, and year ending now. Custom end time is not supported.

3. Click **Apply** and select the required graphs.

4. Hover over different sections of the graph to view more information for the selected time period.
For example, if you select **Last 2 hours**, the baseline period is the 2 hours prior to the selected time range. View the CPU, memory, and session trend over the last 2 hours and the baseline time. If you select **Last month**, the baseline period is the previous month. Select to view the Average IOPS and disk latency over the last month and the baseline time.

1. Click **Export** to export the resource utilization data for the selected period. For more information, see Export reports section in Monitor Deployments.

2. Below the graphs, the table lists the top 10 processes based on CPU or memory utilization. You can sort by any of the columns, which show Application Name, User Name, Session ID, Average CPU, Peak CPU, Average Memory, and Peak Memory over the selected time range. The IOPS and Disk Latency columns cannot be sorted.

   Note:
   The session ID for system processes is displayed as “0000”.

3. To view the historical trend on the resource consumption of a particular process, drill into any of the Top 10 processes.

**Machine Console access**

You can access the consoles of Desktop and Multi-session OS machines hosted on XenServer Version 7.3 and later directly from Monitor. This way, you don’t require XenCenter to troubleshoot issues on XenServer hosted VDAs. For this feature to be available, the XenServer hosting the machine must be of Version 7.3 or later and must be accessible from the Monitor.
To troubleshoot a machine, click the **Console** link in the corresponding Machine Details panel. After authentication of the host credentials you provide, the machine console opens in a separate tab using noVNC, a web-based VNC client. You now have keyboard and mouse access the console.

**Note:**
- This feature is not supported on Internet Explorer 11.
- If the mouse pointer on the machine console is misaligned, see [CTX230727](#) for steps to fix the issue.
- Console access is launched on a new tab, ensure that your browser settings allow pop-ups.
- For security reasons, Citrix recommends that you install SSL certificates on your browser.

**Microsoft RDS license health**

You can view the status of Microsoft RDS license in the Machine Details panel in the **Machine Details** and the **User Details** page for Multi-session OS machines.
One of the following messages is displayed:

- License available
- Not configured properly (warning)
- License error (error)
- Incompatible VDA version (error)

Note:
The RDS license health status for machines under grace period with valid license displays a **License available** message in green. Renew your license before they expire.

For warning and error messages, hover over the info icon to view additional information as given in the following table.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Messages in Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>Available for VDAs version 7.16 and later.</td>
</tr>
<tr>
<td>Error</td>
<td>New RDS connections are not allowed.</td>
</tr>
</tbody>
</table>
### Troubleshoot user issues

June 12, 2019

Use the Monitor’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.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Messages in Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Error</strong></td>
<td>RDS licensing has exceeded its grace period.</td>
</tr>
<tr>
<td><strong>Error</strong></td>
<td>A License Server is not configured for the required OS level with the Per Device Client Access licensing type.</td>
</tr>
<tr>
<td><strong>Error</strong></td>
<td>The configured License Server is incompatible with the RDS Host OS level with the Per Device Client Access licensing type.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>Personal Terminal Server is not a valid RDS licensing type in a Citrix Virtual Apps and Desktops deployment.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>Remote Desktop for Administration is not a valid licensing type in a Citrix Virtual Apps and Desktops deployment.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>An RDS licensing type is not configured.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>The Domain Controller or License Server is unreachable with the Per User Client Access RDS licensing type.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>With the Per Device Client Access licensing type, the Client Device license could not be determined since the license server for the required OS level is unreachable.</td>
</tr>
</tbody>
</table>

**Note:**

This feature is applicable only for Microsoft RDS CAL (Client Access License).
Troubleshooting tips

<table>
<thead>
<tr>
<th>User issue</th>
<th>Suggestions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon takes a long time or fails intermittently or repeatedly</td>
<td>Diagnose user logon issues</td>
</tr>
<tr>
<td>Session startup takes a long time or fails intermittently or repeatedly</td>
<td>Diagnose session startup issues</td>
</tr>
<tr>
<td>Application is slow or won’t respond</td>
<td>Resolve application failures</td>
</tr>
<tr>
<td>Connection failed</td>
<td>Restore desktop connections</td>
</tr>
<tr>
<td>Session is slow or not responding</td>
<td>Restore sessions</td>
</tr>
<tr>
<td>Video is slow or poor quality</td>
<td>Run HDX channel system reports</td>
</tr>
</tbody>
</table>

Note:
To make sure that the machine is not in maintenance mode, from the User Details view, review the Machine Details panel.

Search tips

Search for username is conducted across all configured Active Directories.

When you type a multiuser machine name in a Search field, the Machine Details for the specified machine is displayed.

When you type an endpoint name in a Search field, the unauthenticated (anonymous) and authenticated sessions that are connected to a specific endpoint are listed. This 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 Monitor tab.
Diagnose user logon issues

June 26, 2019

Use Logon Duration data to troubleshoot user logon issues.

Logon duration is measured only for initial connections to a desktop or app using HDX. This data does not include users trying to connect with Remote Desktop Protocol or reconnect from disconnected sessions. Specifically, logon duration is not measured when a user initially connects using a non-HDX protocol and reconnects using HDX.

In the User Details view, the duration is displayed as a number value below which the time the logon occurred is displayed and a graph of the phases of the logon process.

As users logon to Citrix Virtual Apps and Desktops, the Monitor Service tracks the phases of the logon process from the time the user connects from Citrix Workspace app to the time when the desktop is ready to use.

The large number on the left is the total logon time and is calculated by combining the time spent establishing the connection and obtaining a desktop from the Delivery Controller with the time spent to authenticate and logon to a virtual desktop. The duration information is presented in seconds (or fractions of seconds).

Prerequisites

Ensure that the following prerequisites are met for logon duration data and drilldowns to appear:

1. Install Citrix User Profile Manager and Citrix User Profile Manager WMI Plugin on the VDA.
2. Ensure that the Citrix Profile Management Service is running.
3. For XenApp and XenDesktop Sites 7.15 and earlier, disable the GPO setting, Do not process the legacy run list.
4. Audit process tracking must be enabled for Interactive Session drilldown.
5. For GPO drilldown, increase the size of Group Policy operational logs.

Note:

Logon duration is supported only on default Windows shell (explorer.exe) and not on custom shells.

Steps to troubleshoot user logon issues

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.
Citrix Virtual Apps and Desktops service

- 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. Examine the phases of the logon process.

**Logon process phases**

**Brokering**

Time taken to decide which desktop to assign to the user.

**VM start**

If the session required a machine start, this is the time taken to start the virtual machine.

**HDX connection**

Time taken to complete the steps required in setting up the HDX connection from the client to the virtual machine.

**Authentication**

Time taken to complete authentication to the remote session.

**GPOs**

If Group Policy settings are enabled on the virtual machines, this is the time taken to apply group policy objects during logon. The drill-down of the time taken to apply each policy as per the CSEs (Clients-Side Extension) is available as a tooltip when you hover on the GPO bar.
Click **Detailed Drilldown** to see a table with the policy status, and the corresponding GPO name. The time durations in the drilldown represent the CSE processing time only and do not add up to the total GPO time. You can copy the drill-down table for further troubleshooting or use in reports. The GPO time for the policies is retrieved from Event Viewer logs. The logs can get overwritten depending on the memory allocated for the operational logs (default size is 4 MB). For more information about increasing the log size for the operational logs, see the Microsoft technet article [Configuring the Event Logs](https://docs.microsoft.com/en-us/troubleshoot/windows-server/administration/configuring-the-event-logs).

**Logon scripts**

If logon scripts are configured for the session, this is the time taken for the logon scripts to be executed.

**Profile load**

If profile settings are configured for the user or the virtual machine, this is the time taken for the profile to load.

If Citrix Profile Management is configured, the Profile Load bar includes the time taken by Citrix Profile Management to process user profiles. This information helps administrators to troubleshoot high profile processing duration issues. When Profile Management is configured, an increased duration is displayed by the Profile Load bar. This increase is caused by this enhancement and does not reflect a performance degradation. This enhancement is available on VDAs 1903 and later.

Hovering over the Profile Load bar displays a tooltip showing the user profile details for the current session. This additional information can help troubleshoot high profile load issues.
Click **Detailed Drilldown** to drilldown further into each individual folder in the profile root folder (for instance, C:/Users/username), its size and the number of files (including files inside nested folders).

Profile drilldown is available on VDAs 1811 and later. Using the profile drilldown information, you can resolve issues involving a high profile load time. You can:

- Reset the user profile
- Optimize the profile by removing unwanted large files
- Reduce the number of files to reduce the network load
- Use profile streaming

By default, all folder names are visible. To hide the folder names, edit the registry values on the VDA machine using the following steps:
Warning:
Adding and editing the registry 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.

1. On the VDA, add a new registry value `ProfileFoldersNameHidden` at `HKEY_LOCAL_MACHINE\Software\Citrix\Director`.
2. Set the value to 1. This value must be a DWORD (32-bit) value. Folder names visibility is now disabled.
3. To make the folder names visible again, set the value to 0.

Note:
You can use GPO or PowerShell to apply the registry value change on multiple machines. For more information about using GPO to deploy registry changes, see the blog.

Additional information
- Profile drilldown does not consider redirected folders.
- NTUser.dat files in the root folder may not be visible to end users. However, they are included in the profile drilldown and displayed in the list of files in `Root Folder`.
- There are some hidden files in AppData folder which are not included in profile drilldown.
- Number of files and profile size data may not match with the data in the Personalization panel due to certain Windows limitations.

Interactive Session

This is the time taken to “hand off” keyboard and mouse control to the user after the user profile has been loaded. It is normally the longest duration out of all the phases of the logon process and is calculated as: \[ \text{Interactive Session duration} = \text{Desktop Ready Event Timestamp (EventId 1000 on VDA)} - \text{User Profile Loaded Event Timestamp (EventId 2 on VDA)} \]. Interactive Session has three subphases: Pre-userinit, Userinit, and Shell. Hovering over Interactive Session displays a tooltip showing the subphases, the time taken for each subphase, the total cumulative time delay between these subphases, and a link to the documentation.

Note:
This feature is available on VDAs 1811 and later. If you have launched sessions on Sites earlier than 7.18 and then upgraded to 7.18, a ‘Drilldown unavailable due to server error’ message is displayed. However, if you have launched sessions after upgrade, no error message is displayed.

To view the time duration of each subphase, enable Audit process tracking on the VM (VDA). When the Audit process tracking is disabled (default), the time duration of Pre-userinit and the combined time
duration of Userinit and Shell are displayed. You can enable Audit process tracking through a Group Policy Object (GPO) as follows:

1. Create a new GPO and edit it using the GPO editor.
3. On the right pane, double-click **Audit process tracking**.
4. Select **Success** and click Ok.
5. Apply this GPO to the required VDAs or Group.

For more information about Audit process tracking and enabling or disabling it, see **Audit process tracking** in the Microsoft documentation.

Logon Duration panel in the User Details view.

- **Interactive Session – Pre-userinit**: This is the segment of Interactive Session which overlaps with Group Policy Objects and scripts. This subphase can be reduced by optimizing the GPOs and scripts.
- **Interactive Session – Userinit**: When a user logs on to a Windows machine, Winlogon runs userinit.exe. Userinit.exe runs logon scripts, re-establishes network connections, and then starts Explorer.exe, the Windows user interface. This subphase of Interactive Session represents the duration between the start of Userinit.exe to the start of the user interface for the virtual desktop or application.
- **Interactive Session – Shell**: In the previous phase, Userinit starts the initialization of Windows user interface. The Shell subphase captures the duration between the initialization of the user interface to the time user receives keyboard and mouse control.
- **Delay**: This is the cumulative time delay between the **Pre-userinit and Userinit** subphases and the **Userinit and Shell** subphases.

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 can result in a longer logon duration than the
Citrix Virtual Apps and Desktops service

The total logon time does not include the ICA idle time that is the time between the ICA file download and the ICA file launch for an application.

To enable the automatic opening of ICA file upon application launch, configure your browser for automatic ICA file launch upon download of an ICA file. For more information, see CTX804493.

Note:
The Logon Duration graph shows the logon phases in seconds. Any duration values below one second are displayed as sub-second values. The values above one second are rounded to the nearest 0.5 second. The graph has been designed to show the highest y-axis value as 200 seconds. Any value greater than 200 seconds is shown with the actual value displayed above the bar.

**Troubleshooting tips**

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 might 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.

Examine unusual differences, including:

- Missing (current) logon bars
- Major discrepancy between the current duration and this user’s average duration. Causes include:
  - A new application was installed.
  - An operating system update occurred.
  - Configuration changes were made.
  - Profile size of the user is high. In this case, the Profile Load will be high.
- 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.

**Diagnose session startup issues**

September 16, 2019
Citrix Virtual Apps and Desktops service

In addition to the logon process phases mentioned in the Diagnose user logon issues section, Monitor displays the session startup duration. This is divided into the Workspace App Session Startup duration and the VDA Session Startup duration on the User Details and Endpoint Details pages. These two durations further contain individual phases whose startup durations are also displayed. This data helps you to understand and troubleshoot high session startup duration. Further, the time duration for each phase involved in the session startup helps in troubleshooting issues associated with individual phases. For example, if the Drive Mapping time is high, you can check to see whether all the valid drives are mapped correctly in the GPO or script.

Prerequisites

Ensure that the following prerequisites are met for session startup duration data to be displayed:

- VDA 1903 or later.
- Citrix End User Experience Monitoring (EUEM) service must be running on the VDA.

Limitations

The following limitations apply when Monitor displays the session startup duration data:

- Session startup duration is available only for HDX sessions.
- For session launches from iOS and Android OS, only VDA Startup Duration is available.
- IFDCD is available only when Workspace App is detected while launching from a browser.
- For session launches from Mac OS, IFDCD is available for Workspace App 1902 and later only.
- For session launches from Windows OS, IFDCD is available for Workspace app 1902 and later. For earlier versions, IFDCD is displayed for only app launches from browser with Workspace app detected.

Notes:

- If you face issues in the sessions startup duration display after the prerequisites are met, view the Monitor server and VDA logs as described in CTX130320.
- For shared sessions (multiple applications launched in same session), the Workspace App Startup metrics are displayed for the latest connection or the latest application launch.
- Some metrics in VDA Session Startup are not applicable on reconnects. In such cases, a message is displayed.
Citrix Virtual Apps and Desktops service

**Workspace App session startup phases**

**Session Startup Client Duration (SSCD)**

When this metric is high, it indicates a client-side issue that is causing long start times. Review subsequent metrics to determine the probable root cause of the issue. This starts as close as possible to the time of the request (mouse click) and ends when the ICA connection between the client device and VDA has been established. In the case of a shared session, this duration is much smaller, as much of the setup costs associated with the creation of a new connection to the server are not incurred. At the next level down, there are several detailed metrics available.

**ICA File Download Duration (IFDCD)**

This is the time taken for the client to download the ICA file from the server. The overall process is as follows:

1. The user clicks a resource (application or desktop) on the Workspace Application.
2. A request from the user is sent to StoreFront through Citrix Gateway (if configured), which sends the request to the Delivery Controller.
3. The Delivery Controller finds an available machine for the request and sends the machine information and other details to StoreFront. Also, StoreFront requests and receives a one-time ticket from Secure Ticket Authority.
4. StoreFront generates an ICA File and sends it to the user via Citrix Gateway (if configured).

IFDCD represents the time it takes for the complete process (steps 1-4). The IFDCD duration stops counting when the client receives the ICA file.

LPWD is the StoreFront component of the process.

If IFDCD is high (but LPWD is normal), the server-side processing of the launch was successful, but there were communication issues between the client device and the StoreFront. This results from network issues between the two machines. So you could troubleshoot potential network issues first.

**Launch Page Web Server Duration (LPWD)**

This is the time taken to process the launch page (launch.aspx) on the StoreFront. If LPWD is high, there might be a bottleneck on the StoreFront.

Possible causes include:

- High load on the StoreFront. Try to identify the cause of slowdown by checking the Internet Information Services (IIS) logs and monitoring tools, Task Manager, Performance Monitor and so on.
Citrix Virtual Apps and Desktops service

- StoreFront is having issues communicating with other components such as Delivery Controller. Check if the network connection between StoreFront and Delivery Controller is slow or some Delivery Controllers are down or overloaded.

**Name Resolution Web Server Duration (NRWD)**

This is the time taken by the Delivery Controller to resolve the name of a published application/desktop to a VDA Machine IP Address.

When this metric is high, it indicates that the Delivery Controller is taking a long time to resolve the name of a published application to an IP address. Possible causes include a problem on the client, issues with the Delivery Controller, such as the Delivery Controller being overloaded, or a problem with the network link between them.

**Ticket Response Web Server Duration (TRWD)**

This duration indicates the time it takes to get a ticket (if necessary) from the Secure Ticket Authority (STA) Server or Delivery Controller. When this duration is high, it indicates that the STA server or the Delivery Controller are overloaded.

**Session Look-up Client Duration (SLCD)**

This duration represents the time taken to query every session to host the requested published application. The check is performed on the client to determine whether an existing session can handle the application launch request. The method used depends on whether the session is new or shared.

**Session Creation Client Duration (SCCD)**

This duration represents the time taken to create a session, from the moment wfica32.exe (or a similar equivalent file) is launched to the time when the connection is established.

**VDA session startup phases**

**Session Startup VDA Duration (SSVD)**

This duration is the high-level server-side connection start-up metric that indicates the time VDA takes to perform the entire start-up operation. When this metric is high, it indicates that there is a VDA issue increasing session start times. This includes the time spent on the VDA performing the entire start-up operation.
Citrix Virtual Apps and Desktops service

**Credentials Obtention VDA Duration (COVD)**

The time taken for the VDA to obtain the user credentials.

This duration could be artificially inflated if a user fails to provide credentials in a timely manner, and thus, not included in the VDA Startup Duration. This time is likely to be a significant only if manual login is being used and the server side credentials dialog is displayed (or if a legal notice is displayed before login commences).

**Credentials Authentication VDA Duration (CAVD)**

This is the time taken by the VDA to authenticate the user’s credentials against the authentication provider, which could be Kerberos, Active Directory, or a Security Support Provider Interface (SSPI).

**Group Policy VDA Duration (GPVD)**

This duration is the time taken to apply group policy objects during logon.

**Login Script Execution VDA Duration (LSVD)**

This is the time taken by the VDA to run the user’s login scripts.

You can make the user or group’s login scripts asynchronous. Optimize any application compatibility scripts or use environment variables instead.

**Profile Load VDA Duration (PLVD)**

This is the time taken by the VDA to load the user’s profile.

If this duration is high, review your User Profile configuration. Roaming profile size and location contribute to slow session starts. When a user logs on to a session where Terminal Services roaming profiles and home folders are enabled, the roaming profile contents and access to that folder are mapped during logon, which takes extra resources. Sometimes, this can consume significant amount of the CPU usage. Use the Terminal Services home folders with redirected personal folders to mitigate this problem. In general, use Citrix Profile Management to manage user profiles in Citrix environments. If you are using Citrix Profile Management and have slow logon times, check if your antivirus software is blocking the Citrix Profile Management tool.
Citrix Virtual Apps and Desktops service

**Printer Creation VDA Duration (PCVD)**

This is the time taken for the VDA to map the user’s client printers synchronously. If the configuration is set for printer creation to be performed asynchronously, no value is recorded for PCVD as it does not impact completion of the session startup.

Excessive time spent in mapping printers is often the result of the printer auto creation policy settings. The number of printers added locally on the users’ client devices and your printing configuration can directly affect your session start times. When a session starts, Citrix Virtual Apps and Desktops have to create every locally mapped printer on the client device. Reconfigure your printing policies to reduce the number of printers that get created, specifically when users have many local printers. To do this, edit the Printer Auto creation policy in Delivery Controller and Citrix Virtual Apps and Desktops.

**Drive Mapping VDA Duration (DMVD)**

This is the time taken by the VDA to map the user’s client drives, devices, and ports.

Ensure that your base policies include settings to disable unused virtual channels, such as audio or COM port mapping, to optimize the ICA protocol and improve overall session performance.

**Application/Desktop Launch VDA Duration (ALVD/DLVD)**

This phase is a combination of userinit and Shell duration. When a user logs on to a Windows machine, Winlogon runs userinit.exe. Userinit.exe runs logon scripts, re-establishes network connections, and then starts explorer.exe, the Windows User interface. userinit represents the duration between the start of userinit.exe to the start of the user interface for the virtual desktop or application. The Shell duration is the time between the initialization of the user interface to the time user receives keyboard and mouse control.

**Session Creation VDA Duration (SCVD)**

This time includes miscellaneous delays in session creation on VDA.

**Shadow users**

March 15, 2019

Use the shadow user feature to view or work directly on a user’s virtual machine or session. You can shadow both Windows or and Linux VDAs. 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.
Citrix Virtual Apps and Desktops service

Shadowing is launched in a new tab, update your browser settings to allow pop-ups from the Citrix Cloud URL.

Access the shadowing feature from the User Details view. Select the user session, and click Shadow in the Activity Manager view or the Session Details panel.

**Shadowing Linux VDAs**

Shadowing is available for Linux VDAs Version 7.16 or and later running the RHEL7.3 or Ubuntu Version 16.04 Linux distributions.

Note:

- Monitor uses FQDN to connect to the target Linux VDA. Ensure that the Monitor client can resolve the FQDN of the Linux VDA.
- The VDA must have the python-websockify and x11vnc packages installed.
- noVNC connection to the VDA uses the WebSocket protocol. By default, ws:// WebSocket protocol is used. For security reasons, Citrix recommends that you use the secure wss:// protocol. Install SSL certificates on each Monitor client and Linux VDA.

Follow the instructions in Session Shadowing to configure your VDA for shadowing.

1. After you click Shadow, the shadowing connection initializes and a confirmation prompt appears on the user device.
2. Instruct the user to click Yes to start the machine or session sharing.
3. The administrator can only view the shadowed session.

**Shadowing Windows VDAs**

Windows VDA sessions are shadowed using Windows Remote Assistance. Enable User Windows Remote Assistance feature while installing the VDA. For more information, see the Enable or Disable features section in Install VDAs.

1. After you click Shadow, the shadowing connection initializes and a dialog box prompts you to open or save the .msrc incident file.
2. Open the incident file with the Remote Assistance Viewer, if not already selected by default. A confirmation prompt appears on the user device.
3. Instruct the user to click Yes to start the machine or session sharing.
4. 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.

**Send messages to users**

March 15, 2019

From Monitor, 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 logoffs 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. If the user’s machine is connected, the message appears there.

If the message is not sent successfully, an error message appears. Troubleshoot the problem according to the error message. When you have finished, type the subject and message text again and click Try again.

**Resolve application failures**

June 19, 2019

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 grayed out, contact an administrator with the permission to enable the tab.

The list includes only those applications that were launched within the session.

For Multi-session OS machines and Single session OS machines, applications are listed for each disconnected session. If the user is not connected, no applications are displayed.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End the application that is not responding</td>
<td>Choose the application that is not responding and click End Application. Once the application is terminated, ask the user to launch it again.</td>
</tr>
<tr>
<td>End processes that are not responding</td>
<td>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.</td>
</tr>
<tr>
<td>Restart the user’s machine</td>
<td>For Single session 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 Multi-session OS machines, the restart option is not available. Instead, log off the user and let the user log on again.</td>
</tr>
<tr>
<td>Put the machine into maintenance mode</td>
<td>If the machine’s image needs maintenance, such as a patch or other updates, put the machine into maintenance mode. From the Machine Details view, click Details and turn on the maintenance mode option. Escalate to the appropriate administrator.</td>
</tr>
</tbody>
</table>
**Restore desktop connections**

**March 15, 2019**

From Monitor, 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that the machine is not in maintenance mode</td>
<td>On the User Details page, make sure maintenance mode is turned off.</td>
</tr>
<tr>
<td>Restart the user’s machine</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Restore sessions**

**June 19, 2019**

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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End applications or processes that are not responding</td>
<td>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.</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect the Windows session</td>
<td>Click Session Control and then select Disconnect. This option is available only for brokered Multi-session OS machines. For non-brokered sessions, the option is disabled.</td>
</tr>
<tr>
<td>Log off the user from the session</td>
<td>Click Session Control and then select Log Off.</td>
</tr>
</tbody>
</table>

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.

**Run HDX channel system reports**

March 15, 2019

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. To do this, in the HDX panel, click Download System Report.

**Reset a user profile**

March 18, 2019
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 is deleted (for example, the registry is reset and application settings might be deleted).

1. From Monitor, 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 back on. 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.

The preceding steps assume you are using Citrix Virtual Desktops (Desktop VDA). If you are using Citrix Virtual Desktops (Server VDA) you 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 Monitor or using the PowerShell SDK), Monitor first identifies the user profile in use and issues an appropriate reset command. Monitor receives the information through Profile management, including information about the profile size, type, and logon timings.

This diagram illustrates the process following the user log on, when a user profile is reset.

The reset command issued by Monitor 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).

1. If a local profile is present, it is deleted.
2. The network profile is renamed.
3. 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 normally. If a roaming profile is used for the reset, any registry settings in the roaming profile are preserved in the reset profile. 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.
Delegated Administration and Monitoring

June 21, 2019

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.

Administrative permissions determine the monitoring 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.

Monitoring now supports delegated administrator roles that allow you to assign custom defined or built-in roles to administrators. The role determines the available permissions and hence, how an administrator uses monitoring. You can also define the scope applicable for those roles. The scope defines the objects for which the role is applicable.

For information about creating delegated administrators, see the main Delegated Administration article.

The built-in roles and permissions also determine how administrators use Monitor:

<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Permissions in Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Administrator</td>
<td>Full access to all views and can perform all commands, including shadowing a user’s session, enabling maintenance mode, and exporting trends data.</td>
</tr>
<tr>
<td>Delivery Group Administrator</td>
<td>Full access to all views and can perform all commands, including shadowing a user’s session, enabling maintenance mode, and exporting trends data.</td>
</tr>
<tr>
<td>Read Only Administrator</td>
<td>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.</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Permissions in Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk Administrator</td>
<td>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 Single session OS Machines. Cannot access the Dashboard, Trends, Alerts, or Filters views. Cannot use power control options for Multi-session OS machines.</td>
</tr>
<tr>
<td>Machine Catalog Administrator</td>
<td>Can access only the Machine Details page (Machine-based search).</td>
</tr>
<tr>
<td>Host Administrator</td>
<td>No access. This administrator is not supported for Monitor and cannot view data.</td>
</tr>
<tr>
<td>Probe Agent Administrator</td>
<td>Read-only access to Applications page, cannot access any other view. Specifically meant to run the Citrix Probe Agent on endpoint machines.</td>
</tr>
<tr>
<td>Monitoring Full Administrator</td>
<td>Has full access to all views and commands in the Monitor tab</td>
</tr>
</tbody>
</table>

To assign a role (built-in or custom) to a user, from Citrix Cloud menu, go to **Identity and Access Management > Administrators**. Here, when you add or edit access of an administrator, you can select Custom Access and one of the listed roles.
You can define custom roles and scopes in Manage → Citrix Studio → Configuration → Administrators. The built-in roles and custom roles are listed for selection with custom scope.
Citrix Virtual Apps and Desktops service

- Cloud Administrator, All
- Delivery Group Administrator, All
- Delivery Group Administrator, rds1DGAAndCatalog
- Delivery Group Administrator, vdaDGOnly
- Full Monitor Administrator, All - Access to 'Monitor' tab only
- Full Monitor Administrator, rds1DGAAndCatalog - Access to 'Monitor' tab only
- Full Monitor Administrator, vdaDGOnly - Access to 'Monitor' tab only
- Help Desk Administrator, All - Access to 'Monitor' tab only
- Help Desk Administrator, rds1DGAAndCatalog - Access to 'Monitor' tab only
- Help Desk Administrator, vdaDGOnly - Access to 'Monitor' tab only
- Host Administrator, All
- Host Administrator, rds1DGAAndCatalog
- Host Administrator, vdaDGOnly
- Machine Catalog Administrator, All
- Machine Catalog Administrator, rds1DGAAndCatalog
- Machine Catalog Administrator, vdaDGOnly
- Probe Agent Administrator, All
- Probe Agent Administrator, rds1DGAAndCatalog
- Probe Agent Administrator, vdaDGOnly
- Read Only Administrator, All
- Read Only Administrator, rds1DGAAndCatalog
- Read Only Administrator, vdaDGOnly
- TrendsFiltersAndUD, All
- TrendsFiltersAndUD, rds1DGAAndCatalog
- TrendsFiltersAndUD, vdaDGOnly
Data granularity and retention

June 13, 2019

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 the 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 begin-
ning (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 Ser-
vice 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 sched-
ule 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 gran-
ularity 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 that 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.

**Granularity and retention**

The granularity of aggregated data retrieved by Monitor 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
- $T > 30$ days uses per-day granularity

Requested data that does not come from aggregated data comes from the raw Session and Connection
Citrix Virtual Apps and Desktops service 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.

Citrix Virtual Apps and Desktops service supports historical data retention only for 90 days. Hence, one-year trends and reports in Monitor show the last 90 days of data. Data older than 90 days will be stored for a period 2 years for backup and recovery.

<table>
<thead>
<tr>
<th>Setting name</th>
<th>Affected grooming</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GroomSessionsRetent</td>
<td>Session and Connection records retention after Session termination</td>
<td>90</td>
</tr>
<tr>
<td>2 GroomFailuresReten</td>
<td>MachineFailureLog and ConnectionFailureLog records</td>
<td>90</td>
</tr>
<tr>
<td>3 GroomLoadIndexesRe</td>
<td>LoadIndex records</td>
<td>90</td>
</tr>
<tr>
<td>4 GroomDeletedReten</td>
<td>Machine, Catalog, DesktopGroup, and Hypervisor entities that have a LifecycleState of ‘Deleted’. This also deletes any related Session, SessionDetail, Summary, Failure, or LoadIndex records.</td>
<td>90</td>
</tr>
<tr>
<td>5 GroomSummariesReten</td>
<td>DesktopGroupSummary, FailureLogSummary, and LoadIndexSummary records. Aggregated data - daily granularity.</td>
<td>90</td>
</tr>
<tr>
<td>6 GroomMachineHotfixLogRetentionDays</td>
<td>Hotfixes applied to the VDA and Controller machines</td>
<td>90</td>
</tr>
<tr>
<td>Setting name</td>
<td>Affected grooming</td>
<td>Default value</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>GroomMinuteRetentionDays</td>
<td>Aggregated data - minute granularity</td>
<td>3</td>
</tr>
<tr>
<td>GroomHourlyRetentionDays</td>
<td>Aggregated data - hourly granularity</td>
<td>32</td>
</tr>
<tr>
<td>GroomApplicationInstanceRetentionDays</td>
<td>Application Instance history</td>
<td>90</td>
</tr>
<tr>
<td>GroomNotificationLogRetentionDays</td>
<td>Log records</td>
<td>90</td>
</tr>
<tr>
<td>GroomResourceUsageRetentionDays</td>
<td>Resource utilization data - raw data</td>
<td>1</td>
</tr>
<tr>
<td>GroomResourceUsageMinuteRetentionDays</td>
<td>Summary data - minute granularity</td>
<td>7</td>
</tr>
<tr>
<td>GroomResourceUsageHourRetentionDays</td>
<td>Summary data - hour granularity</td>
<td>30</td>
</tr>
<tr>
<td>GroomResourceUsageDayRetentionDays</td>
<td>Summary data - day granularity</td>
<td>90</td>
</tr>
<tr>
<td>GroomProcessUsageRawDataRetentionDays</td>
<td>Process utilization data - raw data</td>
<td>1</td>
</tr>
<tr>
<td>GroomProcessUsageMinuteDataRetentionDays</td>
<td>Summary data - minute granularity</td>
<td>3</td>
</tr>
<tr>
<td>GroomProcessUsageHourDataRetentionDays</td>
<td>Summary data - hour granularity</td>
<td>7</td>
</tr>
<tr>
<td>GroomProcessUsageDayDataRetentionDays</td>
<td>Summary data - day granularity</td>
<td>30</td>
</tr>
<tr>
<td>GroomSessionMetricsDataRetentionDays</td>
<td>Session metrics data</td>
<td>7</td>
</tr>
<tr>
<td>GroomMachineMetricDataRetentionDays</td>
<td>Machine metrics data</td>
<td>3</td>
</tr>
<tr>
<td>GroomApplicationErrorsRetentionDays</td>
<td>Application error data</td>
<td>1</td>
</tr>
</tbody>
</table>
### Setting name Affected grooming Default value

| 23 | GroomApplicationFault Application failure data | 1 |

**Caution:**
Modifying values on the Monitor Service database requires restarting the service for the new values to take effect. To make changes to the Monitor Service database contact 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 (100 K 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.

### Citrix Gateway

February 8, 2019

**Citrix Gateway Service**

Citrix Gateway provides users with secure VPN access to Citrix Virtual Apps and Desktops applications across a range of devices including laptops, desktops, thin clients, tablets, and smartphones.

Citrix Gateway Service enables secure, remote access to Citrix Virtual Apps and Desktops applications, without having to deploy Citrix Gateway in the DMZ or reconfigure your firewall. The entire infrastructure overhead of using Citrix Gateway moves to the cloud and hosted by Citrix.

You enable Citrix Gateway Service in Citrix Cloud. After enabling the service, users can access their VDAs from outside their network, as shown in the following diagram.
Enable or disable the Citrix Gateway service

1. Sign in to Citrix Cloud.
2. In the upper left menu, select Workspace Configuration. The Service Integrations tab indicates whether or not each service is enabled.
3. Use the ellipsis menu on the row containing the service name to select Enable or Disable.

Known issues

- The Citrix Gateway service is enabled for use with HDX traffic as part of the Virtual Apps and Desktops service only. Other Citrix Gateway functionality is not enabled.
- The Citrix Cloud Connector located in your Citrix Cloud resource location communicates with Citrix-managed cloud services communicating through the internet. This communication channel does not support authentication at outbound proxies for access to the internet.
- All network traffic is protected by SSL, but to provide the Citrix Gateway functionality, HDX traffic is present in memory in an unencrypted form.
- SmartAccess does not work for sessions connected through the Citrix Gateway service.

More information

Citrix Gateway product documentation

Citrix VPX

- Deploy a Citrix ADC VPX instance on AWS: This document provides relevant information and instructions for deploying a Citrix ADC VPX instance on AWS.
- Deploy a Citrix ADC VPX instance on Microsoft Azure: This document provides relevant information and instructions for deploying a Citrix ADC VPX instance on Azure.
Citrix Virtual Apps and Desktops service

- **Install a Citrix ADC VPX instance on Citrix Hypervisor (XenServer):** This document provides relevant information and instructions for installing and configuring a Citrix ADC VPX instance on Citrix Hypervisor (XenServer).

For information about Citrix VPX deployments on other hypervisors, see Deploying Citrix VPX.

**SDKs and APIs**

July 10, 2019

**Citrix Virtual Apps and Desktops Remote PowerShell SDK**

The Remote PowerShell (PS) SDK automates complex and repetitive tasks. It provides the mechanism to set up and manage the Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) environment without having to use the Studio user interface.

The supported snap-ins are listed in Limitations. That section also lists the cmdlets that are disabled.

**How this SDK differs from the Citrix Virtual Apps and Desktops Delivery Controller SDK**

In a Citrix Virtual Apps and Desktops deployment that is fully installed and managed by customer administrators, those administrators run cmdlets and scripts in a Site containing both VDAs and Delivery Controllers within a common domain structure. In contrast, the Citrix Virtual Apps and Desktops service splits the VDAs and Controllers into a resource location and the control plane, respectively. This split means the original Citrix Virtual Apps and Desktops PS SDK will not work in a Citrix Virtual Apps and Desktops service environment, because it cannot cross the secure resource location to control plane boundary.

The solution is the Citrix Virtual Apps and Desktops Remote PS SDK. When run in the resource location, the Remote PS SDK accesses the control plane as if it were local, providing the same functionality as a single Citrix Virtual Apps and Desktops site. There is only the lowest non-visible communication layer, enhanced to work either in a single local site or in the cloud environment. The cmdlets are the same, and most existing scripts will work unchanged.

The `Get-XdAuthentication` cmdlet provides the authorization to cross the secure resource location to control plane boundary. By default, `Get-XdAuthentication` prompts users for CAS credentials, and must be done once per PowerShell session. Alternatively, the user can define an authentication profile using an API access Secure Client, created in the Citrix Cloud console. In both cases, the security information persists for use in subsequent PS SDK calls. If this cmdlet is not explicitly executed, it is called by the first PS SDK cmdlet.
Install and use the Remote PowerShell SDK

Requirements:

- Ensure that PowerShell 3.0 or later is available on the machine.
- If the machine has the Citrix Virtual Apps and Desktops Delivery Controller SDK installed, remove that SDK (from Windows Programs and Features) before installing the Remote PowerShell SDK.

To install the Remote PowerShell SDK:

1. Download the installer: https://download.apps.cloud.com/CitrixPoshSdk.exe. The package contains both x86 and x64 implementations.
2. In the downloaded folder, locate and run the installer.
3. Follow the dialogs to complete the installation.

Installation logs are created in %TEMP%\CitrixLogs\CitrixPoshSdk. Logs can help resolve installation issues.

Run the Citrix Virtual Apps and Desktops Remote PS SDK on a domain-joined computer within that resource location:

- Open a PowerShell command prompt. You do not need to run as an administrator.
- Add the Citrix snapins: `asnp citrix.*`.
- You can explicitly authenticate by using the `Get-XdAuthentication` cmdlet. Or, execute your first Citrix Virtual Apps and Desktops PS SDK command, which will prompt you for the same authentication as `Get-XdAuthentication`.
- To bypass the authentication prompt, you can use the `Set-XdCredentials` cmdlet to create a default authentication profile, using a Secure Client created in the Citrix Cloud console.
- Continue executing PS SDK cmdlets or PS SDK automation scripts. See an example below.

Citrix recommends that you do not run this SDK’s cmdlets on Cloud Connectors. The SDK’s operation does not involve the Cloud Connectors.

Uninstall:

From the Windows feature for removing or changing programs, select **Citrix Virtual Apps and Desktops Remote PowerShell SDK**. Right-click and select **Uninstall**. Follow the dialog.

Example activities

Common activities include setting up machine catalogs, applications, and users. A sample script is shown below.

```
1 $users = "xd.local\Domain Users"
2```

© 1999-2019 Citrix Systems, Inc. All rights reserved.
$TSVDACatalogName = "TSVDA"

$TSVDAGName = "TSVDA"

$TSVDMachineName = "xd\ds-tsvda2"

# Create TSVDA Catalog

$brokerUsers = New-BrokerUser -Name $users

$catalog = New-BrokerCatalog -Name $TSVDACatalogName -AllocationType "Random" -Description $TSVDACatalogName -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -SessionSupport "MultiSession" -MachinesArePhysical $true

# Add TSVDA Machine to Catalog

$BrokeredMachine = New-BrokerMachine -MachineName $TSVDMachineName -CatalogUid $catalog.uid

# Create new desktops & applications delivery group

$dg = New-BrokerDesktopGroup -Name $TSVDAGName -PublishedName $TSVDAGName -DesktopKind "Shared" -SessionSupport "MultiSession" -DeliveryType DesktopsAndApps -Description $TSVDAGName

# Create notepad application

New-BrokerApplication -ApplicationType HostedOnDesktop -Name "Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg

# Assign users to desktops and applications

New-BrokerEntitlementPolicyRule -Name $TSVDAGName -DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description $TSVDAGName


New-BrokerAppEntitlementPolicyRule -Name $TSVDAGName -DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description $TSVDAGName

# Add machine to delivery group
Limitations

The following Citrix Virtual Apps and Desktops PowerShell snap-ins are supported in this release:

- Broker
- Active Directory (AD) Identity
- Machine Creation
- Configuration
- Configuration Logging
- Host
- Delegated Administration
- Analytics

For details about cmdlets in those snap-ins, see Citrix Virtual Apps and Desktops SDK.

Once authenticated, remote access remains valid in the current PowerShell session for 24 hours. After this time, you must enter your credentials.

The Remote PS SDK must be run on a computer within the resource location.

The following cmdlets are disabled in remote operations to maintain the integrity and security of the Cloud control plane.

**Citrix.ADIdentity.Admin.V2:**

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Test-AcctDBConnection

**Citrix.Analytics.Admin.V1:**

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
Citrix Virtual Apps and Desktops service

- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

**Citrix.DelegatedAdmin.Admin.V1:**

- Add-AdminRight
- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

**Citrix.Broker.Admin.V2:**

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
Citrix Virtual Apps and Desktops service

- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- Set-BrokerSite
- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

Citrix.Configuration.Admin.V2:

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

Citrix.Host.Admin.V2:
Citrix Virtual Apps and Desktops service

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

**Citrix.ConfigurationLogging.Admin.V1:**

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

**Citrix.MachineCreation.Admin.V2:**

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceConfigurationData
- Set-ProvServiceMetadata
- Test-ProvDBConnection

**Citrix.EnvTest.Admin.V1:**
Citrix Virtual Apps and Desktops service

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

**Citrix.Monitor.Admin.V1:**

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

**Citrix.Storefront.Admin.V1:**

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

**Citrix Virtual Apps and Desktops discovery module for App-V packages**

The Citrix Virtual Apps and Desktop service can deliver applications contained in App-V packages to your end points using the single admin management method. The process of registering App-V packages with the App Library using the Citrix Virtual Apps and Desktop service is slightly different to registering packages using an on-premises deployment. However, the process of assigning applications
Citrix Virtual Apps and Desktops service

to users and launching them on a user’s end point is identical.

The service management console in Citrix Cloud cannot see files in a resource location, and it cannot discover App-V packages on your infrastructure directly. The discovery module contains PowerShell functions you can run on a machine in your resource location to discover App-V packages, and the apps they contain, and push that information to the Citrix Virtual Apps and Desktop Service.

Install and use the discovery module for App-V packages

Requirements:

- Ensure that PowerShell 3.0 or later is available on the machine.
- Ensure that the Citrix Virtual Apps and Desktops Remote PowerShell SDK is installed on the machine.

To install the discovery module for App-V packages:

Download the signed PowerShell module file Citrix.Cloud.AppLibrary.Admin.v1.psm1: Citrix Virtual Apps and Desktops download page. (This file is also provided on the Citrix Virtual Apps and Desktops ISO in Support\Tools\Scripts where it can be copied locally or referenced directly from the CD drive.)

The module contains the following high level functions which you can call from your own PowerShell script:

- **Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>**
  
  Discovers and uploads to the Citrix Virtual Apps and Desktop service all the information necessary to publish applications from a single App-V Package.

- **Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>**
  
  Discovers the UNC paths of packages published by the Management Server and calls Import-AppVPackageToCloud for each one in turn.

  Note:

  Packages discovered in this way are loaded to the Citrix Virtual Apps and Desktops Service using the single admin management method. The Citrix Virtual Apps and Desktops Service cannot deliver packages using the dual admin management method.

Run the discovery module for App-V packages on a domain-joined computer within that resource location:

- Open a PowerShell command prompt. You do not need to run as an administrator.
- Add the Citrix snap-ins: asnp citrix.*.
- You can explicitly authenticate by using the Get-XdAuthentication cmdlet. Or, execute your first discovery module for App-V PS SDK command, which prompts you for the same authentication as Get-XdAuthentication.
Citrix Virtual Apps and Desktops service

- To bypass the authentication prompt, you can use the Set-XdCredentials cmdlet to create a default authentication profile, using a Secure Client created in the Citrix Cloud console.
- Continue executing PS SDK cmdlets or PS SDK automation scripts. See the following examples.

Example activities

**Import the Virtual Apps and Desktops service App-V package discovery module**

```powershell
import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

**Loop through the App-V Package store directory and upload each package**

```powershell
Get-ChildItem -Path "\\FileServer.domain.net\App-V Packages" -Filter *.appv |
Foreach-Object{
    Import-AppVPackageToCloud -PackagePath $_.FullName
}
```

**Discover and upload packages registered with a Microsoft App-V management server**

```powershell
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVManagementServer.domain.net
```

**Read PowerShell help documentation included in the module**

```powershell
Get-Help Import-AppVPackageToCloud
```

**Limitations**

- You cannot discover App-V packages on your resource location infrastructure directly from the service management console in Citrix Cloud.
- Packages discovered by this module cannot be loaded to the Citrix Virtual Apps and Desktops Service using the dual admin management method.
Disclaimer

This software / sample code is provided to you “AS IS” with no representations, warranties or conditions of any kind. You may use, modify and distribute it at your own risk. CITRIX DISCLAIMS ALL WARRANTIES WHATSOEVER, EXPRESS, IMPLIED, WRITTEN, ORAL OR STATUTORY, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. Without limiting the generality of the foregoing, you acknowledge and agree that (a) the software / sample code may exhibit errors, design flaws or other problems, possibly resulting in loss of data or damage to property; (b) it may not be possible to make the software / sample code fully functional; and (c) Citrix may, without notice or liability to you, cease to make available the current version and/or any future versions of the software / sample code. In no event should the software / code be used to support of ultra-hazardous activities, including but not limited to life support or blasting activities. NEITHER CITRIX NOR ITS AFFILIATES OR AGENTS WILL BE LIABLE, UNDER BREACH OF CONTRACT OR ANY OTHER THEORY OF LIABILITY, FOR ANY DAMAGES WHATSOEVER ARISING FROM USE OF THE SOFTWARE / SAMPLE CODE, INCLUDING WITHOUT LIMITATION DIRECT, SPECIAL, INCIDENTAL, PUNITIVE, CONSEQUENTIAL OR OTHER DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. You agree to indemnify and defend Citrix against any and all claims arising from your use, modification or distribution of the code.

Monitor Service OData API

In addition to using the Monitor functions 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

For details, see Monitor Service OData API. For instructions to access the Monitor Service API, see Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

Citrix Virtual Apps and Desktops service APIs

The Virtual Apps and Desktops service APIs are available at https://developerv1.cloud.com/_virtual_apps_and_desktops_service/virtual_apps_and_desktops_service.html.