Citrix Virtual Apps and Desktops service
## Contents

- **Citrix Virtual Apps and Desktops service** | 3
- **What’s new** | 11
- **Known issues** | 31
- **Deprecation** | 33
- **System requirements** | 34
- **Limits** | 40
- **Technical security overview** | 42
- **Delivery methods** | 48
- **Install and configure** | 52
- **Get started** | 57
- **Set up resource locations** | 58
- **Microsoft Azure Resource Manager virtualization environments** | 61
- **Citrix Hypervisor virtualization environments** | 72
- **Microsoft System Center Virtual Machine Manager virtualization environments** | 74
- **VMware virtualization environments** | 77
- **Amazon Web Services virtualization environments** | 83
- **Nutanix virtualization environments** | 91
- **Google Cloud Platform virtualization environments** | 92
- **Scale and size considerations for Cloud Connectors** | 110
- **Create and manage connections** | 126
- **Install VDAs** | 137
- **Install VDAs using the command line** | 152
- **Create machine catalogs** | 159
### Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage machine catalogs</td>
<td>175</td>
</tr>
<tr>
<td>Azure Quick Deploy</td>
<td>182</td>
</tr>
<tr>
<td>Create delivery groups</td>
<td>186</td>
</tr>
<tr>
<td>Manage delivery groups</td>
<td>192</td>
</tr>
<tr>
<td>Create application groups</td>
<td>209</td>
</tr>
<tr>
<td>Manage application groups</td>
<td>216</td>
</tr>
<tr>
<td>Remote PC Access</td>
<td>221</td>
</tr>
<tr>
<td>Remove components</td>
<td>231</td>
</tr>
<tr>
<td>User personalization layer</td>
<td>232</td>
</tr>
<tr>
<td>Upgrade</td>
<td>250</td>
</tr>
<tr>
<td>Print</td>
<td>252</td>
</tr>
<tr>
<td>HDX</td>
<td>253</td>
</tr>
<tr>
<td>Adaptive transport</td>
<td>263</td>
</tr>
<tr>
<td>Rendezvous protocol</td>
<td>272</td>
</tr>
<tr>
<td>Citrix ICA virtual channels</td>
<td>275</td>
</tr>
<tr>
<td>Double hop in Citrix Virtual Apps and Desktops</td>
<td>285</td>
</tr>
<tr>
<td>Devices</td>
<td>287</td>
</tr>
<tr>
<td>Generic USB devices</td>
<td>289</td>
</tr>
<tr>
<td>Mobile and touch screen devices</td>
<td>289</td>
</tr>
<tr>
<td>Serial ports</td>
<td>293</td>
</tr>
<tr>
<td>Specialty keyboards</td>
<td>298</td>
</tr>
<tr>
<td>TWAIN devices</td>
<td>300</td>
</tr>
<tr>
<td>Webcams</td>
<td>300</td>
</tr>
<tr>
<td>Graphics</td>
<td>302</td>
</tr>
<tr>
<td>Feature</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>HDX 3D Pro</td>
<td>304</td>
</tr>
<tr>
<td>GPU acceleration for Windows multi-session OS</td>
<td>305</td>
</tr>
<tr>
<td>GPU acceleration for Windows single-session OS</td>
<td>307</td>
</tr>
<tr>
<td>Thinwire</td>
<td>312</td>
</tr>
<tr>
<td>Text-based session watermark</td>
<td>319</td>
</tr>
<tr>
<td>Multimedia</td>
<td>320</td>
</tr>
<tr>
<td>Audio features</td>
<td>324</td>
</tr>
<tr>
<td>Browser content redirection</td>
<td>333</td>
</tr>
<tr>
<td>HDX video conferencing and webcam video compression</td>
<td>341</td>
</tr>
<tr>
<td>HTML5 multimedia redirection</td>
<td>345</td>
</tr>
<tr>
<td>Optimization for Microsoft Teams</td>
<td>348</td>
</tr>
<tr>
<td>Monitor, troubleshoot, and support Microsoft Teams</td>
<td>367</td>
</tr>
<tr>
<td>Windows Media redirection</td>
<td>374</td>
</tr>
<tr>
<td>General content redirection</td>
<td>375</td>
</tr>
<tr>
<td>Client folder redirection</td>
<td>376</td>
</tr>
<tr>
<td>Host to client redirection</td>
<td>377</td>
</tr>
<tr>
<td>Local App Access and URL redirection</td>
<td>384</td>
</tr>
<tr>
<td>Generic USB redirection and client drive considerations</td>
<td>393</td>
</tr>
<tr>
<td>Policies</td>
<td>402</td>
</tr>
<tr>
<td>Manage</td>
<td>403</td>
</tr>
<tr>
<td>Autoscale</td>
<td>404</td>
</tr>
<tr>
<td>Configuration logging</td>
<td>435</td>
</tr>
<tr>
<td>Delegated administration</td>
<td>438</td>
</tr>
<tr>
<td>Local Host Cache</td>
<td>451</td>
</tr>
</tbody>
</table>

© 1999-2020 Citrix Systems, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale and size considerations for Local Host Cache</td>
<td>459</td>
</tr>
<tr>
<td>Virtual IP and virtual loopback</td>
<td>477</td>
</tr>
<tr>
<td>Sessions</td>
<td>480</td>
</tr>
<tr>
<td>Tags</td>
<td>487</td>
</tr>
<tr>
<td>Zones</td>
<td>495</td>
</tr>
<tr>
<td>Citrix license usage</td>
<td>504</td>
</tr>
<tr>
<td>User access</td>
<td>504</td>
</tr>
<tr>
<td>Monitor</td>
<td>507</td>
</tr>
<tr>
<td>Site Analytics</td>
<td>508</td>
</tr>
<tr>
<td>Alerts and notifications</td>
<td>516</td>
</tr>
<tr>
<td>Filter data to troubleshoot failures</td>
<td>526</td>
</tr>
<tr>
<td>Monitor historical trends across a site</td>
<td>528</td>
</tr>
<tr>
<td>Monitor Autoscale-managed machines</td>
<td>535</td>
</tr>
<tr>
<td>Troubleshoot deployments</td>
<td>538</td>
</tr>
<tr>
<td>Troubleshoot applications</td>
<td>539</td>
</tr>
<tr>
<td>Application probing</td>
<td>543</td>
</tr>
<tr>
<td>Desktop probing</td>
<td>547</td>
</tr>
<tr>
<td>Troubleshoot machines</td>
<td>552</td>
</tr>
<tr>
<td>Troubleshoot user issues</td>
<td>560</td>
</tr>
<tr>
<td>Diagnose user logon issues</td>
<td>561</td>
</tr>
<tr>
<td>Diagnose session startup issues</td>
<td>568</td>
</tr>
<tr>
<td>Shadow users</td>
<td>573</td>
</tr>
<tr>
<td>Send messages to users</td>
<td>575</td>
</tr>
<tr>
<td>Resolve application failures</td>
<td>575</td>
</tr>
</tbody>
</table>

© 1999-2020 Citrix Systems, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore desktop connections</td>
<td>577</td>
</tr>
<tr>
<td>Restore sessions</td>
<td>577</td>
</tr>
<tr>
<td>Run HDX channel system reports</td>
<td>578</td>
</tr>
<tr>
<td>Reset a user profile</td>
<td>579</td>
</tr>
<tr>
<td>Feature compatibility matrix</td>
<td>581</td>
</tr>
<tr>
<td>Delegated administration and monitoring</td>
<td>584</td>
</tr>
<tr>
<td>Data granularity and retention</td>
<td>589</td>
</tr>
<tr>
<td>Citrix Virtual Apps and Desktops service for Citrix Service Providers</td>
<td>594</td>
</tr>
<tr>
<td>Citrix Gateway service</td>
<td>600</td>
</tr>
<tr>
<td>SDKs and APIs</td>
<td>601</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

July 27, 2020

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, 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 the Cloud Connectors.

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. The **Local Host Cache** feature requires a customer-managed StoreFront in each resource location (zone).

**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

**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 plug-ins 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:
• 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*.

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 in the product documentation 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

- 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.

To learn about feature availability in various Citrix Virtual Apps and Desktops offerings, see the Citrix Virtual Apps and Desktops Release Feature Matrix. This information can be helpful in hybrid deployments.

Get started

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

What’s new

August 20, 2020

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).

Important:

If the Personal vDisk (PvD) component was ever installed on a VDA, that VDA cannot be upgraded to version 1912 LTSR or later. To use the new VDA, you must uninstall the current VDA and then install the new VDA. (This instruction applies even if you installed PvD but never used it.) For details, see Important notice about upgrading VDAs.

August 2020

New and enhanced features

Support for two new Citrix Virtual Apps and Desktops service editions. Citrix Monitor now supports two new Citrix Virtual Apps and Desktops service editions, namely, Citrix Virtual Apps Advanced service and Citrix Virtual Apps and Desktops Advanced service. For more information, see the Citrix Monitor Feature compatibility matrix.

Support for shared Virtual Private Cloud (VPC) in Google Cloud Platform. The Citrix Virtual Apps and Desktop service supports Shared VPC on Google Cloud Platform as a host resource. You can use Machine Creation Services (MCS) to provision machines in a Shared VPC and manage them using Citrix Studio. For information about Shared VPC, see Shared Virtual Private Cloud.

Zone selection support for Google Cloud Platform. The Citrix Virtual Apps and Desktops service supports zone selection on Google Cloud Platform to enable sole tenancy. Sole tenancy provides exclusive access to a sole tenant node, which is a physical compute engine server dedicated to hosting only your project’s VMs.

Sole Tenant nodes allow you to group your VMs together on the same hardware or separate your VMs from other project’s VMs. These nodes can help you meet dedicated hardware requirements for Bring Your Own License (BYOL) scenarios. Sole Tenant nodes enable you to comply with network access control policy, security and privacy requirements such as HIPAA. You can create VMs in desired locations where Sole Tenant nodes are allocated. For configuration information, see Enable sole tenancy.
Note:
Sole tenancy is the only route to using Windows 10 VDI deployments on Google Cloud. Server VDI also supports this method. A detailed description for sole tenancy can be found on the Google documentation site.

**Improved boot performance for Azure system disks.** This release supports improved boot performance for Citrix Cloud implementations using Azure when MCSIO is enabled. With this support, you can retain the system disk. This provides the following advantages:

- VMs and applications now boot and launch with performance similar to how the golden image is served.
- Reduction in API quota consumption, deleting and creating the system disk, and state transition delay caused when you delete a VM.

For configuration information, see Improve boot performance.

**July 2020**

**New and enhanced features**

**Support for granular, role-based access to the Filters page.** Citrix Studio now provides more granular control over access to the Monitor > Filters page when you create a custom role. Specifically, you can assign permissions to view any combination of Machines, Sessions, Connections, and Application Instances to a custom role. The following are four additional options for the Director object in the Create Role window:

- View Filters page - Application Instances only
- View Filters page - Connections only
- View Filters page - Machines only
- View Filters page - Sessions only

For information about creating roles, see Create and manage roles. This feature is being rolled out in phases. It might not yet be activated for your account.

**Power-off delay support for assigned VDI machines (PowerShell only).** In earlier releases, the power-off delay applied only to unassigned machines. Starting with this release, the power-off delay applies to both assigned and unassigned machines. For more information, see How Autoscale power manages machines.

**Support for Windows Client licenses.** The Citrix Virtual Apps and Desktops service now supports using Windows Client licenses to provision VMs in Azure. To run Windows 10 VMs in Azure, verify that your volume licensing agreement with Microsoft qualifies for this usage. For more information, see Create a machine catalog using an Azure Resource Manager master image.
May 2020

New and enhanced features

**Machine restart schedules.** You can now indicate whether a restart schedule affects machines that are in maintenance mode. This feature is available only in PowerShell. For details, see Scheduled restarts for machines in maintenance mode.

**Resource availability.** You can now ensure resource availability during an outage without having to publish resources in every zone (resource location). For details, see Resource availability.

April 2020

New and enhanced features

**Enhanced scheduling granularity for VDI Delivery Groups (PowerShell only).** Autoscale now supports defining the peak times for the days included in a schedule at a granular level of 30 minutes. You can set the minimum number of machines running in a VDI Delivery Group separately for each half hour of the day. Also, Autoscale can now scale up or down the number of powered-on machines in VDI Delivery Groups on a half-hourly basis instead of on an hourly basis. For more information, see Broker PowerShell SDK commands.

**MTU Discovery.** The Citrix protocol Enlightened Data Transport (EDT) now has MTU Discovery capabilities. MTU Discovery allows EDT to automatically determine and set the payload size for the session. This feature enables the ICA session to adjust to networks with non-standard Maximum Transmission Unit (MTU) or Maximum Segment Size (MSS) requirements. The ability to adjust avoids packet fragmentation that might result in degraded performance or failure to establish an ICA session. This update requires a minimum of Citrix Workspace app 1911 for Windows. If using Citrix Gateway, the minimum Citrix ADC firmware version required is 13.0.52.24 or 12.1.56.22. For more information, see EDT MTU Discovery.

March 2020

New and enhanced features

**PVS target device metrics.** Citrix Monitor now provides a PVS target device metrics panel on the Machine Details page. Use the panel to view the status of Provisioning target devices for single-session and multi-session OS machines. Several metrics for Network, Boot, and Cache are available on this panel. These metrics help you monitor and troubleshoot PVS target devices to ensure that they are up and running. For more information, see PVS target device metrics.
**AWS instance property capturing.** MCS now reads properties from the instance from which the AMI was taken and applies the IAM role and tags of the machine to the machines provisioned for a given catalog. When using this optional feature, the catalog creation process finds the selected AMI source instance, reading a limited set of properties. These properties are then stored in an AWS Launch Template, which is used to provision machines for that catalog. Any machine in the catalog inherits the captured instance properties. For more information, see [AWS instance property caching](#).

**AWS operational resource tagging.** This release introduces an option to tag resources created by Citrix components during provisioning. Each tag represents a label consisting of a customer-defined key and an optional value that improve your ability to manage, search for, and filter resources. For more information, see [AWS operational resource tagging](#).

**Secure transfer in Azure storage.** Machine Creation Services (MCS) provides an enhancement for storage accounts created by MCS-provisioned catalogs in Azure Resource Manager environments. This enhancement automatically enables the secure transfer required property. This option enhances storage account security by only allowing requests to the account from secure connections. For more information, see [Require secure transfer to ensure secure connections](#) on the Microsoft site.

Enable the Secure transfer required property when creating a storage account in Azure:

![Create storage account](image)

**Support for Azure SSD managed disks.** Machine Creation Services (MCS) supports standard SSD managed disks for Azure virtual machines. This disk type provides consistent performance, and de-
Citrix Virtual Apps and Desktops service

livers better availability compared to HDD disks. For more information, see Standard SSD Disks for Azure Virtual machine workloads.

Use the PowerShell `StorageAccountType` custom property in the `New-ProvScheme` command or `Set-ProvScheme` command to configure this feature:

```xml
<Property xsi:type='"StringProperty"' Name='"UseManagedDisks"' Value='"true"'/><Property xsi:type='"StringProperty"' Name='"StorageAccountType"' Value='"StandardSSD_LRS"'/><Property xsi:type = '"StringProperty"' Value='"Windows_Server"'/>
```

Note:

This feature is only available when using managed disks, that is, the custom property `UseManagedDisks` is set to `true`. For unmanaged disks only Standard HDD and Premium SSD are supported.

January 2020

New and enhanced features

**Language bar in Citrix Studio.** Starting with this release, Citrix Studio provides a language bar to facilitate correct keyboard mapping.

- If the language of Citrix Cloud or the display language of your browser is set to **English** or **Japanese**, the language bar does not appear.

- If the language of Citrix Cloud or the display language of your browser is set to **German**, **Spanish**, or **French**, the language bar appears after you log on to Citrix Studio. There are two language options on the language bar list. Select an option that matches the topmost language of your browser.

  Tip:

  Settings that you configure for the language bar might not take effect. In this case, log out and log back on.

**Restart schedule maximum delay timer (PowerShell only).** If a scheduled restart of machines in a Delivery Group doesn't begin because of a site database outage, you can specify how long to wait beyond the scheduled start time. If the database connection is restored during that interval, the restarts begin. If the connection isn't restored during that interval, the restarts don't begin. For details, see Scheduled restarts delayed due to database outage.

**Vertical load balancing (PowerShell only).** Previously, the service used horizontal load balancing for all RDS launches, which assigns incoming load to the least-loaded RDS machine. That remains the default. Now, you can use PowerShell to enable vertical load balancing as a site-wide setting.
When vertical load balancing is enabled, the broker assigns incoming load to the most-loaded machine that has not hit a high watermark. This saturates existing machines before moving on to new machines. As users disconnect and free up existing machines, new load is assigned to those machines.

By default, horizontal load balancing is enabled. To view, enable, or disable vertical load balancing, the `Get-BrokerSite` and `Set-BrokerSite` cmdlets now support the `UseVerticalScalingForRdsLaunches` setting. For more information, see Load manage machines in Delivery Groups.

**December 2019**

**New and enhanced features**

**Service for Citrix Service Providers (CSP).** CSPs can now onboard tenant customers to the Virtual Apps and Desktops service, configure customer administrator access to the service, and provide shared or dedicated workspaces to customers' users using federated domains. For more information, see Citrix Virtual Apps and Desktops service for Citrix Service Providers.


**Autoscale.** Autoscale now provides the capability to create machines and delete them dynamically. You can leverage the capability by using a PowerShell script. The script helps you dynamically scale up or down the number of machines in the Delivery Group based on the current load conditions. For more information, see Dynamically provision machines with Autoscale.

**November 2019**

**New and enhanced features**

**GroomStartHour.** Monitor now supports GroomStartHour - a new configuration that helps administrators to determine the time of the day that grooming should start running. For more information, see the Citrix Virtual Apps and Desktops SDK documentation.

**OData Pagination.** Monitor now supports OData pagination. All OData v4 endpoints return a maximum of 100 records per page with a link to the next 100 records in the response. For more information, see Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud.
October 2019

New and enhanced features

**App-V.** App-V functionality is now available in Citrix Cloud. You can add App-V packages to the Delivery Controller in your Citrix Cloud configuration, in either single- or dual admin mode. The *Virtual Apps and Desktops Service App-V package discovery module*, available in Citrix Downloads, allows you to import App-V packages and register Microsoft App-V servers. The apps they contain are then available to your users. This PowerShell module allows you to register Microsoft App-V Management and Publishing Servers using DNS URLs, avoiding the need for servers behind load balancing mechanisms to be registered using their actual machine URL. For more information, see [Citrix Virtual Apps and Desktops service discovery module for App-V packages and servers](https://docs.citrix.com/en-us/virtualapps-and-desktops/citrix-cloud.html).


September 2019

New and enhanced features

**VDA support for Windows Virtual Desktop.** For supported operating systems and VDA versions see [Virtual Delivery Agents (VDAs) in a Windows Virtual Desktop environment](https://docs.citrix.com/en-us/virtualapps-and-desktops/citrix-cloud.html).

**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 more information, see [Power manage VDI machines transitioning to a different time period with disconnected sessions](https://docs.citrix.com/en-us/virtualapps-and-desktops/citrix-cloud.html).

**Machine catalogs: Tags.** You can now use PowerShell to apply tags to machine catalogs. For more information, see [Tags on machine catalogs](https://docs.citrix.com/en-us/virtualapps-and-desktops/citrix-cloud.html).

**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 more information, 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:
Citrix Virtual Apps and Desktops service

- 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 it to an item, you can tailor certain operations to apply to only items that have a specified tag. For more information, 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 more information, see TLS versions. For comprehensive guidance, seeCTX247067.

**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 more information, 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 tool tip 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 multi-session OS (formerly 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
Citrix Virtual Apps and Desktops service

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 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-](https://www.citrix.com/about/citrix-product-).
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.
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 in VDAs 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.

**Copied!**

**Failed!**

**Known issues**

July 30, 2020

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

• The drop-down arrow icon for the Average IOPS, Session Control, and Power Control buttons might not appear on the **User Details** and the **Machine Details** pages. However, the functionality works as expected. To view all the items on the menu, click anywhere on the button. [DIR-11875]
- 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]

- Changing the name of an AWS Virtual Private Cloud (VPC) in the AWS console breaks the existing hosting unit in Citrix Cloud. When the hosting unit is broken, you cannot create new catalogs or add machines to existing catalogs. [PMCS-7701]

- When you try to use the ‘Restart’ option in Workspace App web or desktop, the ‘Restarting’ dialogue never closes and never reports success. The hypervisor will show the machine has shut down but has not started. As a workaround, after some time the user can close the ‘Restarting’ dialogue and launch the desktop and the desktop will start. [BRK-5564]

- When you deploy machines in an MCS catalog, the provisioning task can fail and the following error message appears: “Terminating Error: Desktop Studio closed.” The error details might show that no AD accounts were created. The catalog might complete successfully at a later time without intervention. The issue is seen in large, complex deployments. [PMCS-8869]

- In Citrix Studio, you might encounter the following language bar issues:
  - If the language of Citrix Cloud or the display language of your browser is set to German, Spanish, or French, the language bar might not appear. The issue occurs if the topmost language of your browser does not match the language of Citrix Cloud or the display language of your browser. To work around the issue, move the display language of your browser to the top. Log out and log back on. For Google Chrome users, to set the language as the topmost language, navigate to Settings > Advanced > Languages, click the vertical ellipsis next to the applicable language, and then select Move to the top.
  - If the language of Citrix Cloud or the display language of your browser is set to German, Spanish, or French:
    - The language bar might not work as expected. For example, if you press Alt + numbers on the numeric keypad, the target symbol appears twice. For example, if you press Alt + 65, two A characters appear.
    - And if you select that language option in the language bar after you log on to Citrix Studio and then attempt to type in an input box, the language option in the language
bar might switch to the default. To work around the issue, switch the language option back.

– If the language of Citrix Cloud is set to **English (US)** or the display language of your browser is set to **English**, the language bar might still appear. The issue occurs when the topmost language of your browser is not **English**. To work around the issue, move the display language of your browser to the top. Log out and log back on.

– If you click the minus sign (-) to minimize the language bar, you can no longer get the language bar back. To work around the issue, log out and log back on.

– If you change the language of Citrix Cloud to a language that is not on the language bar list, the language appears on the language bar list. If you select that language in the language bar, the keyboard might not work as expected. To work around the issue, select a language from the language bar that matches the topmost language of your browser.

– If the language of Citrix Cloud is set to **Japanese**, you might not be able to type some characters. To work around the issue, set the display language of your browser to **English (US)**, change the local keyboard layout to **English (US)**, log out of Citrix Studio, and log back on. [STUD-8819]

For issues related to current VDAs, see **Known issues**.

**Copied!**

**Failed!**

**Deprecation**

**August 12, 2020**

This article gives you advanced notice of Citrix Virtual Apps and Desktops service features that are being phased out, so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when features are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality. For details about product lifecycle support, see the **Product Lifecycle Support Policy** article.

**Note:**

Citrix Virtual Apps and Desktops deprecations and removals are described in their own **Deprecation** article.
Citrix Virtual Apps and Desktops service

**Deprecations and removals**

The following list shows the Citrix Virtual Apps and Desktops service features that are deprecated or removed.

*Deprecated* items are not removed immediately. Citrix continues to support them but they will be removed in a future release.

*Removed* items are removed, or no longer supported, in the Citrix Virtual Apps and Desktops service. Dates in **bold** face indicate the latest updates.

<table>
<thead>
<tr>
<th>Item</th>
<th>Deprecation announced in release</th>
<th>Removed in release</th>
<th>Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to import Citrix Provisioning target devices to create catalogs in cloud Studio.</td>
<td>August 2020</td>
<td>Use the Citrix Provisioning Export Devices Wizard to push Citrix Provisioning VMs into Delivery Controllers/MCS for catalog creation.</td>
<td></td>
</tr>
</tbody>
</table>

*Copied!*

*Failed!*

**System requirements**

July 16, 2020

**Introduction**

System requirements for components that are not covered here (such as 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 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 VM is based on the hardware and not the user workloads (except for RAM; you 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). For VDA installation guidance, see:

- Install VDAs
- Install VDAs using the command line.

### Cloud Connectors

For details, see Cloud Connector Installation.

### Virtual Delivery Agents (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
- Windows Server 2016
- Windows Server 2019

Supported VDA versions:

- On supported Windows 10 and Windows Server: VDA 1909 or newer supported versions
- On Windows 7: VDA 7.15.5000 (version 7.15 with Cumulative Update 5) or newer supported 7.15 CUs

Citrix supports Windows 2008 R2, using VDA 7.15.5000 (version 7.15 with Cumulative Update 5) or newer supported 7.15 CUs. Using this OS requires the appropriate Microsoft Windows Server and RDS licensing, if needed.

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

### VDA for single-session OS

The following information applies to the latest VDA release.
**Citrix Virtual Apps and Desktops service**

**Supported operating systems:**

- Windows 10
  - For edition support, see [CTX224843](#). That article also contains links to Citrix known issues with the supported Windows versions.
  - Desktop composition redirection and legacy graphics mode are not supported on Windows 10.

**Requirements:**

- Microsoft .NET Framework 4.8 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 single-session VDA on Windows Server 2016. See [Server VDI](#) for guidance.

For information about installing a VDA on a Windows 7 machine, see [Earlier operating systems](#).

See also Virtual Delivery Agents (VDAs) in a Windows Virtual Desktop environment.

### VDA for multi-session OS

The following information applies to the latest VDA release.

**Supported operating systems:**

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

The installer automatically deploys the following requirements:

- Microsoft .NET Framework 4.8 is installed automatically, if it (or a later version) is not already installed.
Citrix Virtual Apps and Desktops service


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.

See also Virtual Delivery Agents (VDAs) in a Windows Virtual Desktop environment.

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 2019
- Windows Server 2016

Requirements:

- Microsoft Visual C++ 2017 Runtime, 32-bit and 64-bit
- Microsoft .NET Framework 4.8 (minimum)

For multi-session VDAs, 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**

For supported StoreFront versions, see the [StoreFront system requirements](#).

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.

For details about resource limits in a deployment, see [Limits](#).
Limits

August 14, 2020

The values in this article indicate the limits of a single Citrix Virtual Apps and Desktops service instance. When the number of concurrent users exceeds 75,000, Citrix can scale out and combine multiple Citrix Virtual Apps and Desktops service instances, to deliver a unified experience at any scale.

Configuration limits

The following table lists the limits for site-level resources.

If policies exceed the limit, Citrix recommends using the Workspace Environment Management service or Active Directory Group Policy Objects (GPOs).

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory domains</td>
<td>25</td>
</tr>
<tr>
<td>Application folders</td>
<td>1,000</td>
</tr>
<tr>
<td>Application Groups</td>
<td>250</td>
</tr>
<tr>
<td>Applications</td>
<td>2,000</td>
</tr>
<tr>
<td>Catalogs</td>
<td>500</td>
</tr>
<tr>
<td>Delivery Groups</td>
<td>500</td>
</tr>
<tr>
<td>Host connections</td>
<td>40</td>
</tr>
<tr>
<td>Hosting units per connection</td>
<td>40</td>
</tr>
<tr>
<td>Resource locations</td>
<td>25</td>
</tr>
<tr>
<td>Studio policies</td>
<td>100</td>
</tr>
<tr>
<td>Tags</td>
<td>500</td>
</tr>
<tr>
<td>VDAs</td>
<td>40,000</td>
</tr>
</tbody>
</table>

Resource location limits

The following table lists the limits for each resource location.

If your requirements exceed these limits, Citrix recommends using additional resource locations.
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-session VDAs</td>
<td>5,000</td>
</tr>
<tr>
<td>Multi-session VDAs</td>
<td>500</td>
</tr>
<tr>
<td>Active Directory domains</td>
<td>1</td>
</tr>
<tr>
<td>Host connections</td>
<td>10</td>
</tr>
</tbody>
</table>

**Machine Creation Services (MCS) limits**

The MCS limits in the following table are the recommended maximums for a single public provider subscription.

You are likely to reach quota limits from your public cloud vendor at lower levels. In such cases, contact the vendor to raise your subscription quota. For larger-scale deployments, Citrix recommends a hub-and-spoke model, where VDAs are distributed across multiple subscriptions and host connections.

For more information, see the following reference architectures:

- Citrix Virtual Apps and Desktops Service on Azure
- Reference Architecture for Citrix Virtual Apps and Desktops on AWS

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDAs per Amazon Web Services account per region</td>
<td>1,500</td>
</tr>
<tr>
<td>VDAs per Google Cloud Platform project</td>
<td>500</td>
</tr>
<tr>
<td>VDAs per Microsoft Azure subscription</td>
<td>1,200</td>
</tr>
</tbody>
</table>

**Usage limits**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent Director full administrators</td>
<td>5</td>
</tr>
<tr>
<td>Concurrent Director help desk administrators</td>
<td>50</td>
</tr>
<tr>
<td>Concurrent end users</td>
<td>75,000</td>
</tr>
<tr>
<td>Concurrent Studio cloud administrators</td>
<td>50</td>
</tr>
<tr>
<td>Concurrent Studio help desk administrators</td>
<td>60</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources published to a single user</td>
<td>250</td>
</tr>
<tr>
<td>Session launches per minute</td>
<td>2,000</td>
</tr>
</tbody>
</table>

Technical security overview

August 20, 2020

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.

- **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 Virtual Apps and Desktops service

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 CTX-101810 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.
The XML trust setting applies to deployments that use:

- An on-premises StoreFront.
- A subscriber (user) authentication technology that does not require passwords. Examples of such technologies are domain pass-through, smart cards, SAML, and Veridium solutions.

Enabling the XML trust setting allows users to successfully authenticate and then start applications. The Cloud Connector trusts the credentials sent from StoreFront. Enable this setting only when you have secured communications between your Citrix Cloud Connectors and StoreFront (using firewalls, IPsec, or other security recommendations).

This setting is disabled by default.

Use the Citrix Virtual Apps and Desktops Remote PowerShell SDK to manage the XML trust setting.

- To check the XML trust setting’s current value, run `Get-BrokerSite` and inspect the value of `TrustRequestsSentToTheXMLServicePort`.
- To enable XML trust, run `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`
- To disable XML trust, run `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`

### 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>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Receiver</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<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.](https://www.citrix.com/downloads/workspace-app/)

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](https://www.citrix.com/security) 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](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.

- **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 ma-
Chine 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

June 26, 2020

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 know what to expect.

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.

Sign up

Sign up for a Citrix account and request a Citrix Virtual Apps and Desktops service demo.

Set up a resource location (Connect to infrastructure)

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

How-to:

- Set up a resource location
- Video about installing Cloud Connectors:
Create a connection to the resource location

After you add a resource location, create a connection from the service's control plane to the resource location.

For a simple proof of concept deployment, this step isn't necessary.

Install VDAs (Register resources)

Each machine that delivers applications and desktops to users must have a Citrix Virtual Delivery Agent (VDA) installed on it.

- For a simple proof of concept deployment, download and install a VDA on one machine.
- If you're using a master image to provision VMs, install a VDA on the master image. Each machine that is provisioned using that master image contains that VDA.
- For a Remote PC Access deployment, install a VDA for single-session OS on each physical office PC. You can use your existing Electronic Software Distribution (ESD) methods.

How-to:

- Installation preparation and instruction
• Command-line VDA installation details

• Video about downloading and installing a VDA:

Create a machine catalog (Create collection of resources)

After you create a connection to your resource location, the service’s Manage workflow guides you to create a machine catalog. A catalog contains machines that deliver apps or desktops to your users.

For a full deployment, you can use Citrix tools to provision a machine catalog containing multiple machines of the same type. You can create a master image on your hypervisor or cloud service to be used for the provisioning. The master image contains apps or desktops, and a VDA. That image is used to provision machines in the catalog.

How-to:

• Create a machine catalog

• If you are using Azure Resource Manager to host your resources, you can optionally use the Azure Quick Deploy deployment method. For details, see Azure Quick Deploy.

• Video about creating a machine catalog in a full deployment:
Create a delivery group (Assign users)

After you create your first machine catalog, the Manage 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.

How-to:

- Create a delivery group
- 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.

How-to:

- 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. The **Access** tab contains the Workspace URL. For more information, see **Citrix Workspace**.
  - From the Citrix Virtual Apps and Desktops service **Welcome** page, the workspace URL appears at the bottom of the page.
- For information about Workspace configuration, see **Citrix Workspace**.
- Video about launching applications and desktops from your workspace:
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 demo.
2. Discuss integration requirements with Citrix.
3. Complete settings in the Citrix Cloud portal.

To sign up for a Citrix account and request a demo, contact your Citrix sales representative. When you’re ready to proceed, go to https://onboarding.cloud.com.
After you sign in, in the Citrix Virtual Apps and Desktops service tile, click **Request Demo**. Provide the requested information. A Citrix representative will contact you to discuss your requirements, environment, and plans. Depending on our representative’s assessment, you’ll be authorized to participate in an administrator demo or a proof of concept trial.

While waiting for the demo, you can review the information linked 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 demo, 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 service’s **Manage** console. 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 one of these services, and want to subscribe to this service, you can 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.

Copied!

Failed!

**Set up resource locations**

March 9, 2020
Citrix Virtual Apps and Desktops service

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

- Active Directory domain controller
- Hypervisors or cloud services, known as hosts
- Virtual Delivery Agents (VDAs). VDAs are the machines containing the apps or desktop. Each machine also has a Citrix VDA installed. The term VDA often refers to the VDA software and the machine on which it is installed.
- 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. Then set up Citrix Gateway.
- Citrix StoreFront servers (optional and customer-managed).
- To communicate with Citrix Cloud, every resource location must contain a Citrix Cloud Connector. A minimum of 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. For more information, see Zones.

For more information, see:

- Connect to Citrix Cloud
- Primary 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.
- 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, and 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

© 1999-2020 Citrix Systems, Inc. All rights reserved.
Citrix Virtual Apps and Desktops service

- 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 more information, see:

- Active Directory functional levels
- Active Directory contains Citrix Virtual Apps and Desktops details.
- Identity and access management in Citrix Cloud.

**Cloud Connectors**

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.

- Cloud Connectors functions
- Cloud Connector technical details and requirements
- Cloud Connector proxy and firewall configuration

**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

© 1999-2020 Citrix Systems, Inc. All rights reserved.
Install Cloud Connectors

Install two Cloud Connectors in each resource location. (Only one Cloud Connector is required, but two are recommended.)

For Cloud Connector installation instructions, see Cloud Connector installation.

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.
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. See Name restrictions.

Where to go next

- For a simple proof-of-concept deployment, install a VDA on a machine that will deliver apps or a desktop to your users.
- For a full deployment, create a connection to a resource location.
- Review all the steps in the installation and configuration process

Microsoft Azure Resource Manager virtualization environments

August 26, 2020

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:

Citrix Virtual Apps and Desktops service

- **Service principal:** https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-objects/

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.)

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 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.

**Improve boot performance**

You can improve boot performance for Azure managed disks when MCSIO is enabled. Use the PowerShell `PersistOsDisk` custom property in the `New-ProvScheme` command to configure this feature. Options associated with `New-ProvScheme` include:

```xml
  <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
  <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
  <Property xsi:type="StringProperty" Name="ResourceGroups" Value="benvaldev5RG3" />
  <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
</CustomProperties>
```

To enable this feature, set the `PersistOsDisk` custom property to `true`. For example:
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.’ See CTX219211 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. Rectify this by removing 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 an account to the directory, which takes 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 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 requires 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.
8. 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 must return to that page and select a region that has virtual networks.

9. 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 https://
   $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.
   - 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 must return to that page and select a region that has virtual networks.

6. 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 Create machine catalogs.

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:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/

Select whether to use existing Windows licenses. Using Windows licenses along with Windows images (Azure platform support images or custom images) lets you run Windows VMs in Azure at a reduced cost. There are two types of licenses:

- Windows Server license. Lets you use your Windows Server or Azure Windows Server licenses, allowing you to utilize Azure Hybrid Use Benefits (HUB). For details, see https://azure.microsoft.com/pricing/hybrid-use-benefit/. HUB reduces the cost of running VMs in Azure to the base compute rate, waiving the cost of extra Windows Server licenses from the Azure gallery.


**Note:**

The Windows Client license option varies depending on the operating system you select during machine catalog setup. If you select Multi-session OS, the option appears as Use
my Windows 10 licenses. If you select Single-session OS, the option appears as Use my Windows Client licenses.

You can verify that the provisioned VM is utilizing the licensing benefit by running the following PowerShell command: `Get-AzMRSResourceGroup MyResourceGroup -Name MyVM`.

- For the Windows Server license type, verify that the license type is Windows_Server. More instructions are available at https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.

- For the Windows Client license type, verify that the license type is Windows_Client. More instructions are available at https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Alternatively, you can use the Get-Provscheme PowerShell SDK to perform the verification. For example: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. For more information about this cmdlet, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

Azure Managed Disks are used for VMs in the catalog by default. If you want to use regular storage accounts instead, select 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 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 Azure resource groups.

- 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.
Citrix Virtual Apps and Desktops service

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 the Microsoft documentation.

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
• CTX219211: 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 \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](https://support.citrix.com/article/CTX137465).

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).

Convert Virtual Hard Disk on the root\virtualization\v2 namespace

Example:

```powershell
$ims = Get-WmiObject -class $class -namespace “root\virtualization\v2”;
$result = $ims(ConvertVirtualHardDisk($diskName, $vhdastext)

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.

Create Virtual Hard Disk on the root\virtualization\v2 namespace

Example:

```powershell
$ims = Get-WmiObject -class $class -namespace “root\virtualization\v2”;
$result = $ims.CreateVirtualHardDisk($vhdastext);
```

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 though 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 HyperV machine copies the disk from the SMB storage to local Hyper-V storage through a PowerShell script running in the PowerShell V3 remote session.
2. HCL reads the disk from the Hyper-V machine’s administrator share into memory.
3. HCL deletes the file from the administrator share.

**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](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.
Citrix Virtual Apps and Desktops service

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>
<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>
</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.

### 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.Provisioning.CloneTemplate</td>
<td>Virtual machine &gt; Provisioning &gt; Clone template</td>
</tr>
<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.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>
<tr>
<td>VirtualMachine.Interact.Reset</td>
<td>Virtual machine &gt; Interaction &gt; Reset</td>
</tr>
<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>
</tbody>
</table>
Delete provisioned machines

<table>
<thead>
<tr>
<th>SDK</th>
<th>User interface</th>
</tr>
</thead>
<tbody>
<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>VirtualMachine.Config.RemoveDisk</td>
<td>Virtual machine &gt; Configuration &gt; Remove disk</td>
</tr>
<tr>
<td>VirtualMachine.Inventory.Delete</td>
<td>Virtual machine &gt; Inventory &gt; Remove</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

November 20, 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.
- 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.

**Note:**
Changing the name of an AWS Virtual Private Cloud (VPC) in the AWS console breaks the existing hosting unit in Citrix Cloud. When the hosting unit is broken, you cannot create new catalogs or add machines to existing catalogs. From Known Issue: PMCS-7701

## 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>Select the Public security group.</td>
</tr>
</tbody>
</table>

5. When finished, click **Save**.
### Citrix Virtual Apps and Desktops service

<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:
• 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 cwcconnector.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 %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

August 20, 2020

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 console, 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* page, 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** page, 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 GCP 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, be 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 GCP 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 GCP 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`.
   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
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. Virtual networks with the (Shared) suffix appended to their name represent shared VPCs. If you configure a subnet-level IAM role for a shared VPC, only specific subnets of the shared VPC appear on the subnet list.

   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. To configure the connection, 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 does not 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 comprise 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 do not 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. Use the naming conventions established by GCP when configuring machine catalogs. See **Bucket and object naming guidelines** for more information.

In Citrix Studio, follow the guidance in **Create machine catalogs**. The following description is unique to GCP 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, 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**. If you want to use the sole tenancy functionality, be sure to select an image whose node group property is correctly configured. See **Enable sole tenancy**.

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**. If you use sole tenant node groups for machine catalogs, be sure to select only the zones where reserved sole tenant nodes are available. See **Enable sole tenancy**.

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 enter the sequence of characters representing the naming scheme for the provisioned VM computer accounts created in Active Directory. The account naming scheme can contain 1–64 characters, and cannot contain blank spaces, or non-ASCII or special characters.
   - 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 \ / ; : # # . * = < > | [ ] { } " " ' ( ) .

    Machine catalog creation might take a long time to complete. After that, Studio lists the catalog you created. You can verify that the machines are created on the target node groups in the GCP console.

### 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:

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

You can also power manage 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 multi-session OS 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.

**Shared Virtual Private Cloud**

Shared Virtual Private Clouds (VPCs) comprise a host project, from which the shared subnets are made available, and one or more service projects that use the resource. Shared VPCs are desirable options
for larger installations because they provide centralized control, usage, and administration of shared
corporate Google cloud resources. For more information, see the Google Documentation site.

With this feature, Machine Creation Services (MCS) supports provisioning and managing machine cata-
logs deployed to Shared VPCs. This support, which is functionally equivalent to the support currently
provided in local VPCs, differs in two areas:

1. You must grant additional permissions to the Service Account used to create the Host Connect-
   tion. This process allows MCS to access and utilize Shared VPC Resources.
2. You must create two firewall rules, one each for ingress and egress. These firewall rules are used
during the image mastering process.

New permissions required

A GCP service account with specific permissions is required when creating the host connection. These
additional permissions must be granted to any service accounts used to create Shared VPC based host
connections.

Tip:

These additional permissions are not new to the Citrix Virtual Apps and Desktops service. They
are used to facilitate the implementation of local VPCs. With Shared VPCs, these additional per-
missions allow access to other shared VPC resources.

A maximum of four additional permissions must be granted to the service account associated with
the host connection to support Shared VPC:

1. `compute.firewalls.list` - This permission is mandatory. It allows MCS to retrieve the list of fire-
   wall rules present on the Shared VPC.
2. `compute.networks.list` - This permission is mandatory. It allows MCS to identify the Shared
   VPC networks available to the service account.
3. `compute.subnetworks.list` - This permission is optional depending on how you use VPCs. It
   allows MCS to identify the subnets within the visible Shared VPCs. This permission is already
   required when using local VPCs but must also be assigned in the Shared VPC host project.
4. `compute.subnetworks.use` - This permission is optional depending on how you use VPCs. It
   is necessary to use subnet resources in the provisioned machine catalogs. This permission is
   already required for using local VPCs but must also be assigned in the Shared VPC host project.

When using these permissions, consider that there are different approaches based on the type of per-
mission used to create the machine catalog:

- Project-level permission:
  - Allows access to all Shared VPCs within the host project.
  - Requires the permissions #3 and #4 must be assigned to the service account.
- Subnet-level permission:
Citrix Virtual Apps and Desktops service

- Allows access to specific subnets within the Shared VPC.
- Permissions #3 and #4 are intrinsic to the subnet level assignment and therefore do not need to be assigned directly to the service account.

Select the approach that matches your organizational needs and security standards.

Tip:
For more information about the differences between project-level and subnet-level permissions, see the Google Cloud documentation.

Firewall Rules

During the preparation of a machine catalog, a machine image is prepared to serve as the master image system disk for the catalog. When this process occurs, the disk is temporarily attached to a virtual machine. This VM must run in an isolated environment that prevents all inbound and outbound network traffic. This is accomplished through a pair of deny-all firewall rules; one for ingress and one for egress traffic. When using GCP local VCPs, MCS creates this firewall in the local network and applies it to the machine for mastering. After mastering completes, the firewall rule is removed from the image.

We recommend keeping the number of new permissions required to use Shared VPCs to a minimum. Shared VPCs are higher-level corporate resources and typically have more rigid security protocols in place. For this reason, create a pair of firewall rules in the host project on the shared VPC resources, one for ingress and one for egress. Assign the highest priority to them. Apply a new target tag to each of these rules, using the following value:

citrix-provisioning-quarantine-firewall

When MCS creates or updates a machine catalog, it searches for firewall rules containing this target tag. It then examines the rules for correctness and applies them to the machine used to prepare the master image for the catalog. If the firewall rules are not found, or the rules are found but the rules or their priorities are incorrect, a message similar to the following appears:

"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. "Please ensure you have created 'deny all'firewall rules with the network tag 'citrix-provisioning-quarantine-firewall'and proper priority." "Refer to Citrix Documentation for details."

Configuring the shared VPC

Before adding the Shared VPC as a host connection in Citrix Studio, complete the following steps to add service accounts from the project you intend to provision into:
1. Create an IAM role.
2. Add the service account used to create a CVAD host connection to the Shared VPC host project IAM role.
3. Add the Cloud Build service account from the project you intend to provision into to the Shared VPC host project IAM role.

**Create an IAM role**

Determine the role’s access level — *project level access* or a more restricted model using *subnet level access*.

**Project level access for IAM role.** For the project level IAM role, include the following permissions:

- `compute.firewalls.list`
- `compute.networks.list`
- `compute.subnetworks.list`
- `compute.subnetworks.use`

To create a project level IAM role:

1. In the GCP console, navigate to **IAM & Admin > Roles**.
2. On the **Roles** page, click **CREATE ROLE**.
3. On the **Create Role** page, specify the role name. Click **ADD PERMISSIONS**.
   a) On the **Add permissions** page, add permissions to the role, individually. To add a permission, type the name of the permission in the **Filter table** field. Select the permission and then click **ADD**.
   b) Click **CREATE**.

**Subnet-level IAM role.** This role omits the addition of the permissions `compute.subnetworks.list` and `compute.subnetworks.use` after selecting **CREATE ROLE**. For this IAM access level, the permissions `compute.firewalls.list` and `compute.networks.list` must be applied to the new role.

To create a subnet level IAM role:

1. In the GCP console, navigate to **VPC network > Shared VPC**. The **Shared VPC** page appears, displaying the subnets of the Shared VPC networks that the host project contains.
2. On the **Shared VPC** page, select the subnet that you want to access.
3. In the top-right corner, click **ADD MEMBER** to add a service account.
4. On the **Add members** page, complete these steps:
   a) In the **New members** field, type the name of your service account and then select your service account in the menu.
   b) Click the **Select a role** field and then **Compute Network User**.
c) Click **SAVE**.

5. In the GCP console, navigate to **IAM & Admin > Roles**.

6. On the **Roles** page, click **CREATE ROLE**.

7. On the **Create Role** page, specify the role name. Click **ADD PERMISSIONS**.
   a) On the **Add permissions** page, add permissions to the role, individually. To add a permission, type the name of the permission in the **Filter table** field. Select the permission, and then click **ADD**.
   b) Click **CREATE**.

**Add a service account to the host project IAM role**

After creating an IAM role, perform the following steps to add a service account for the host project:

1. In the GCP console, navigate to the host project and then to **IAM & Admin > IAM**.
2. On the **IAM** page, click **ADD** to add a service account.
3. On the **Add members** page:
   a) In the **New members** field, type the name of your service account and then select your service account in the menu.
   b) Click the Select a role field, type the IAM role you created, and then click the role in the menu.
   c) Click **SAVE**.

The service account is now configured for the host project.

**Add the cloud build service account to the shared VPC**

Every Google Cloud subscription has a service account that is named after the project ID number, followed by `cloudbuild.gserviceaccount`. For example: `705794712345@cloudbuild.gserviceaccount`.

You can determine what the project ID number is for your project by selecting **Home** and **Dashboard** in the Google Cloud console:
Find the **Project Number** below the **Project Info** area of the screen.

Perform the following steps to add the Cloud Build service account to the Shared VPC:

1. In the Google Cloud console, navigate to the host project and then to **IAM & Admin > IAM**.
2. On the **Permissions** page, click **ADD** to add an account.
3. On the **Add members** page, complete these steps:
   a) In the **New members** field, type the name of the Cloud Build service account and then select your service account in the menu.
   b) Click the **Select a role** field, type **Computer Network User**, and then click the role in the menu.
   c) Click **SAVE**.

**Create firewall rules**

As part of the mastering process, MCS copies the selected machine image and uses it to prepare the master image system disk for the catalog. During mastering, MCS attaches the disk to a temporary virtual machine, which then runs preparation scripts. This VM must run in an isolated environment that prohibits all inbound and outbound network traffic. To create an isolated environment, MCS requires two **deny all** firewall rules (an ingress rule and an egress rule). Therefore, create two firewall rules in the **Host Project** as follows:

1. In the GCP console, navigate to the host project and then to **VPC network > Firewall**.
2. On the **Firewall** page, click **CREATE FIREWALL RULE**.
3. On the **Create a firewall rule** page, complete the following:
   - **Name**. Type a name for the rule.
   - **Network**. Select the Shared VPC network to which the ingress firewall rule applies.
   - **Priority**. The smaller the value is, the higher the priority of the rule is. We recommend a small value (for example, 10).
   - **Direction of traffic**. Select **Ingress**.
Citrix Virtual Apps and Desktops service

- **Action on match.** Select Deny.
- **Targets.** Use the default, Specified target tags.
- **Target tags.** Type citrix-provisioning-quarantine-firewall.
- **Source filter.** Use the default, IP ranges.
- **Source IP ranges.** Type a range that matches all traffic. Type 0.0.0.0/0.
- **Protocols and ports.** Select Deny all.

4. Click CREATE to create the rule.
5. Repeat steps 1–4 to create another rule. For **Direction of traffic**, select **Egress**.

Add a connection

After adding the network interfaces to the Cloud Connector instance, add a connection.

Enable sole tenancy

The Citrix Virtual Apps and Desktops service supports sole tenancy. With sole tenancy, you specify the zones where you want to create VMs in Citrix Studio. To configure sole tenancy, you must complete the following on GCP:

- Reserve a sole-tenant node
- Create the VDA master image

Reserving a Google Cloud sole-tenant node

To reserve a sole-tenant node, perform the following steps:

1. In the Google Cloud console, navigate to **Compute Engine > Sole-tenant nodes.**
2. On the **Sole-tenant nodes** page, click **CREATE NODE GROUP.**
3. On the **Create a node group** page, complete these steps:
   a) Type a name for the node group. For example, *mh-sole-tenant-node-group-1.*
   b) Select a region. For example, *us-east1.*
   c) Select a zone where the reserved system resides. For example, *us-east1-b.*
      We recommend that the region and the zone you select allow access to your domain controllers and the subnets used for provisioning machine catalogs.
   d) Associate a node group with a node template. Perform these steps:
      Important:
      A node template is used to indicate performance characteristics of the system that is
reserved in the node group. Those characteristics include the number of vGPUs, the amount of memory allocated to the node, and the machine type used for machines created on the node.

i. Select **Create node template** from the drop-down menu. The **Create a node template** page appears.

ii. On the **Create a node template** page, configure the required information:

- **Name**. Type a name for the node template.
- **Node type**. From the drop-down menu, select a node type that meets your needs. For more information on node types, see the Google Cloud documentation at [https://cloud.google.com/compute/docs/nodes/sole-tenant-nodes#node_types](https://cloud.google.com/compute/docs/nodes/sole-tenant-nodes#node_types).

iii. Click **Create** to exit the **Create a node template** page and to return to the **Create a node group** page.

4. Click **Create** to complete creating a node group.

**Creating the VDA master image**

To deploy machines on the sole-tenant node successfully, you need to take additional steps when creating a master VM image. Machine instances on GCP have a property called **node affinity labels**. Instances used as master images for catalogs deployed to the sole-tenant node require a **node affinity label** that matches the name of the **target node group**. To achieve this, keep the following in mind:

- For a new instance, set the label in the Google Cloud console when creating an instance. For details, see Set a node affinity label when creating a new instance.
- For an existing instance, set the label by using the **gcloud** command line. For details, see Set a node affinity label for an existing instance.

**Note:**

If you intend to use sole tenancy with a shared VPC, see Shared Virtual Private Cloud.

**Set a node affinity label when creating a new instance**

To set the node affinity label:

1. In the GCP console, navigate to **Compute Engine > VM instances**.
2. On the **VM instances** page, click **Create instance**.
3. On the **Instance creation** page, type or configure the required information and then click **management, security, disks, networking, sole tenancy** to open the settings panel.
4. On the **Sole tenancy** tab, click **Browse** to view the available node groups in the current project. The **Sole-tenant node** page appears, displaying a list of available node groups.
5. On the **Sole-tenant node** page, select the applicable node group from the list and then click **Select** to return to the **Sole tenancy** tab. The node affinity labels field populates with the information you selected. This setting ensures that machine catalogs created from the instance will be deployed to the selected node group.

6. Click **Create** to create the instance.

**Set a node affinity label for an existing instance**

To set the node affinity label:

1. In the GCP console, click the terminal icon in the top-right corner to launch the Google Cloud Shell:

   ![Terminal icon](image)

   A terminal window appears at the bottom of the user interface. In the Google Cloud Shell terminal window, use the `gcloud compute instances` command to set a node affinity label. Include the following information in the `gcloud` command:

   - **Name of the VM.** For example, use an existing VM named `s*2019-vda-base.*`  
   - **Name of the node group.** Use the node group name you previously created. For example, `mh-sole-tenant-node-group-1`.
   - **The zone where the instance resides.** For example, the VM resides in the `*us-east-1b` zone.

   For example, type the following command in the terminal window:

   ```bash
   gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"
   ```


2. Navigate to the **VM instance details** page of the instance and verify that the **Node Affinities** field populates with the label.

**Create a machine catalog**

After setting the node affinity label, **configure the machine catalog.**

**More information**

- Connections and resources
Scale and size considerations for Cloud Connectors

March 6, 2020

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.
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
- 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 col-
lected 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 performance. 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)
- **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 con-
Citrix Virtual Apps and Desktops service

trol. 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 VDAs throughout 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.

<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>
</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

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Average Memory Use (MB)</th>
<th>Peak Memory Use (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XaXCloudProxy</td>
<td>800</td>
<td>1,200</td>
</tr>
<tr>
<td>RemoteHCLServer</td>
<td>400</td>
<td>600</td>
</tr>
<tr>
<td>Lsass</td>
<td>200</td>
<td>300</td>
</tr>
<tr>
<td>NetScaler.CloudGateway</td>
<td>100</td>
<td>150</td>
</tr>
<tr>
<td>CloudServices.WebRelayAgent</td>
<td>50</td>
<td>70</td>
</tr>
<tr>
<td>CloudServices.CredentialProvider</td>
<td>30</td>
<td>40</td>
</tr>
<tr>
<td>CloudServices.AgentWatchDog</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>CloudServices.AgentSystem</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>CloudServices.AgentLogger</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>CloudServices.Agent</td>
<td>5</td>
<td>7</td>
</tr>
</tbody>
</table>

- 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.

CPU usage by top components on A2v2 Cloud Connector during 1,000 session launch
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>

© 1999-2020 Citrix Systems, Inc. All rights reserved.
Citrix Virtual Apps and Desktops service

<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>Total login</td>
<td>1,693 ms</td>
<td>1,629 ms</td>
<td>3,406 ms</td>
<td>3,621 ms</td>
</tr>
<tr>
<td>Retrieve ICA file</td>
<td>3,464 ms</td>
<td>3,659 ms</td>
<td>4,730 ms</td>
<td>6,222 ms</td>
</tr>
<tr>
<td>OS logon complete</td>
<td>38.83 seconds</td>
<td>41.91 seconds</td>
<td>37.67 seconds</td>
<td>40.08 seconds</td>
</tr>
<tr>
<td>Total launch</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 ms</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.

<table>
<thead>
<tr>
<th>OS</th>
<th>Machine count</th>
<th>Master image copy</th>
<th>Active directory account creation</th>
<th>Machine creation</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIN 2012 R2</td>
<td>100</td>
<td>4 minutes</td>
<td>3 mins</td>
<td>4 minutes</td>
</tr>
<tr>
<td>WIN 2012 R2</td>
<td>1,000</td>
<td>5 minutes</td>
<td>30 mins</td>
<td>100 minutes</td>
</tr>
<tr>
<td>WIN 10 32-BIT</td>
<td>100</td>
<td>4 minutes</td>
<td>3 mins</td>
<td>4 minutes</td>
</tr>
<tr>
<td>WIN 10 32-BIT</td>
<td>100</td>
<td>4 minutes</td>
<td>3 mins</td>
<td>4 minutes</td>
</tr>
</tbody>
</table>
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.

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-specific articles.

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
Citrix Virtual Apps and Desktops service

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.

*Copied!*

*Failed!*
Install VDAs

July 7, 2020

Important:
If you’re upgrading a VDA that has the Personal vDisk (PvD) component installed, see Important notice about upgrading VDAs.

Introduction

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:
Citrix Virtual Apps and Desktops service

- 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.
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 Microsoft .NET Framework version is installed before beginning the VDA installation.
- For Windows multi-session 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 for the current release 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.
- Browser content redirection.

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

Using VDAWorkstationCoreSetup.exe is equivalent to using the VDAWorkstationSetup.exe installer to install a single-session 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).
Citrix Virtual Apps and Desktops service

Command-line option: \texttt{/masterpvsimage}

• (Appears only on multi-session OS machines) \textbf{Enable brokered connections to a server}: Select this option to install a VDA on a physical or virtual machine that will not be used as a master image.

Command-line option: \texttt{/remotepc}

• (Appears only on multi-session OS machines) \textbf{Enable Remote PC Access}: Select this option to install a VDA on a physical machine for use with Remote PC Access.

Command-line option: \texttt{/remotepc}

Click \textbf{Next}.

This page does not appear:

• If you’re upgrading a VDA.
• If you are using the \texttt{VDAWorkstationCoreSetup.exe} installer.

\textbf{Step 3. Select the components to install and the installation location}

On the \textbf{Core components} page:

• \textbf{Location}: By default, components are installed in \texttt{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: \texttt{/installdir}

• \textbf{Components}: By default, Citrix Workspace app for Windows is not installed with the VDA. If you are using the \texttt{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 `/includeadditional` 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.

<table>
<thead>
<tr>
<th>Additional Components page</th>
<th>Citrix Personalization for App-V</th>
<th>Citrix AppDisk/Personal vDisk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment page: “Master image with MCS” or “Master image with Citrix Provisioning ...” selected</td>
<td>Not selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Environment page: “Enable brokered connections to server” (for multi-session OS) or “Remote PC Access” (for single-session OS) selected</td>
<td>Not selected</td>
<td>Not shown because it’s not valid for this use case.</td>
</tr>
</tbody>
</table>
## Additional Components page

<table>
<thead>
<tr>
<th>Additional Component</th>
<th>Selected/Not selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Supportability tools</td>
<td>Selected/Not selected</td>
</tr>
<tr>
<td>Citrix User Profile Manager</td>
<td>Selected/Not selected</td>
</tr>
<tr>
<td>WMI Plugin</td>
<td>Selected/Not selected</td>
</tr>
<tr>
<td>Citrix Files for Windows</td>
<td>Not selected/Not selected</td>
</tr>
<tr>
<td>Citrix Files for Outlook</td>
<td>Not selected/Not selected</td>
</tr>
</tbody>
</table>

This page does not appear if:

- You are using the `VDAGuestClientCoreSetup.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 Virtual Apps and Desktops service

- **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.
Citrix Virtual Apps and Desktops service

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

[Diagram of Diagnostics page]

© 1999-2020 Citrix Systems, Inc. All rights reserved.
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 24, 2020

**Important:**

If you’re upgrading a VDA that has the Personal vDisk (PvD) component installed, see Important notice about upgrading VDAs.

Introduction

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 from the command line

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 multi-session OS Virtual Delivery Agent, run VDAServerSetup.exe
   - For the single-session OS Virtual Delivery Agent, run VDAWorkstationSetup.exe
   - For the single-session 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 the appropriate command below, using the valid options listed in this article.

   - For VDAServerSetup_XXXX.exe, run <extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe
   - For VDAWorkstationCoreSetup_XXXX.exe, run <extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe
   - For VDAWorkstationSetup_XXXX.exe, run <extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe

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.

- /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 VDA 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, 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 HDX adaptive transport requires, 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, 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 not managed by MCS does not need the Machine Identity Service component. Valid values are:

- 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
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 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.

- /includeadditional component","component" …
  Includes installation of one or more comma-separated optional components, each enclosed in straight quotation marks. The component names are case-sensitive.

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:

- 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
- User personalization layer

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.

• /masterpvsimage
  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 multi-session OS VDA. 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 remount 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 port`

Valid only when the `/reconfig` option is specified. Port number to enable for communications between the VDA and the Controller. The previously configured port is disabled, unless it is port 80.

- `/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 `/portnumber`, `/controllers`, or `/enable_hdx_ports` options. If you specify this option without also specifying the `/quiet` option, the graphical interface for customizing the VDA launches.

- `/remotepc`

Valid only for Remote PC Access deployments (single-session OS) or brokered connections (multi-session 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
- Citrix Supportability Tools
- Citrix Files for Windows
- Citrix Files for Outlook
- User personalization layer
This option is not valid when using the VDAWorkstationCoreSetup.exe installer. That installer automatically excludes installation of these components.

- **/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 single-session OS VDA on a supported Windows server. Omit this option when installing a multi-session VDA 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 multi-session OS. The VDA will be used as a master image.

VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/enable_hdx_ports /masterimage
The following command installs a Core Services VDA on a single-session 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.

Copied!
Failed!

**Create machine catalogs**

July 16, 2020

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.
Citrix Virtual Apps and Desktops service

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.

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 cannot 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 cannot 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.

**AWS dedicated host tenancy support**

You can use MCS to provision AWS dedicated hosts. An administrator can create a catalog of machines with host tenancy defined through PowerShell.

An Amazon [EC2] dedicated host is a physical server with [EC2] instance capacity that is fully dedicated, allowing you to use existing per-socket, or per-VM software licenses.

Dedicated hosts have preset utilization based on instance type. For example, a single allocated dedicated host of C4 Large instance types is limited to running 16 instances. See the [AWS site](http://aws.amazon.com) for more information.

The requirements for provisioning to AWS hosts include:

- An imported BYOL (bring your own license) image (AMI). With dedicated hosts, use and manage your existing licenses.
- An allocation of dedicated hosts with sufficient utilization to satisfy provisioning requests.
- enable auto-placement.

To provision to a dedicated host in AWS using PowerShell, use the `New-ProvScheme` cmdlet with the parameter TenancyType set to Host.

Refer to the [Citrix Developer Documentation](https://docs.citrix.com) for more information.

**AWS instance property capturing**

When you create a catalog to provision machines using Machine Creation Services (MCS) in AWS, you select an AMI to represent the master/golden image of that catalog. From that AMI, MCS uses a snapshot of the disk. In previous releases, if you wanted roles and/or tags on your machines you would use the AWS console to set them individually.

To improve this process, MCS reads properties from the instance from which the AMI was taken and applies the Identity Access Management (IAM) role and tags of the machine to the machines provisioned for a given catalog. When using this optional feature, the catalog creation process finds the selected AMI source instance, reading a limited set of properties. These properties are then stored in an AWS
Citrix Virtual Apps and Desktops service

Launch Template, which is used to provision machines for that catalog. Any machine in the catalog inherits the captured instance properties.

Captured properties include:

- IAM roles – applied to provisioned instances
- Tags - applied to provisioned instances, their disk, and NICs. These tags are applied to transient Citrix resources, including: S3 bucket and objects, volume and worker resources, and AMIs, snapshots, and launch templates.

Tip:
The tagging of transient Citrix resources is optional and is configurable using the custom property `AwsOperationalResourcesTagging`.

Capturing the AWS instance property

You can use this feature by specifying a custom property, `AwsCaptureInstanceProperties`, when creating a provisioning scheme for an AWS hosting connection:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true" ...
```

To use this feature, you must specify a broader set of permissions for the AWS service key. These permissions include:

- `ec2:AssociateIamInstanceProfile`
- `ec2:CreateLaunchTemplate`
- `ec2:DeleteLaunchTemplate`
- `ec2:DeleteTags`
- `ec2:DisassociateIamInstanceProfile`
- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeLaunchTemplateVersions`
- `ec2:DescribeSnapshots`
- `ec2:DescribeTags`
- `iam:PassRole`
- `s3:PutBucketTagging`
- `s3:PutObjectTagging`

Refer to the Citrix Developer Documentation for more information.
AWS operational resource tagging

An Amazon Machine Image (AMI) represents a type of virtual appliance used to create a virtual machine within the Amazon Cloud environment, commonly referred to as EC2. You use an AMI to deploy services that use the EC2 environment. When you create a catalog to provision machines using MCS for AWS, you select the AMI to act as the golden image for that catalog.

Important:
Creating catalogs by capturing an instance property and launch template is required for using operational resource tagging. For details, see the preceding section AWS instance property capturing.

To create an AWS catalog, you must first create an AMI for the instance you want to be the golden image. MCS reads the tags from that instance and incorporates them into the launch template. The launch template tags are then applied to all Citrix resources created in your AWS environment, including:

- Virtual Machines
- VM disks
- VM network interfaces
- S3 buckets
- S3 objects
- Launch templates
- AMIs

Tagging an operational resource

To use PowerShell to tag resources:

1. Open a PowerShell window from the DDC host.
2. Run the command `asnp citrix` to load Citrix-specific PowerShell modules.

To tag a resource for a provisioned VM, use the new custom property `AwsOperationalResourcesTagging`. The syntax for this property is:

```
New-ProvScheme -CustomProperties "‘AwsCaptureInstanceProperties, true; AwsOperationalResourcesTagging, true’ ...<standard provscheme parameters>
```

To use the `AwsOperationalResourcesTagging` custom property, ensure that the following new permissions exist for the AWS service key:

- `ec2:CreateTags`
- `ec2:DeleteTags`
- `ec2:DescribeTags`
- `s3:PutBucketTagging`
Citrix Virtual Apps and Desktops service

- s3:PutObjectTagging

Set these permissions in the IAM section of the AWS Management Console:

1. In the **Summary** panel, select the **Permissions** tab.
2. Click **Add permissions**.

**Add Permissions to** screen, grant permissions:

Use the following as an example in the **JSON** tab:
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 antivirus 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 virtual disk 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.
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 resources 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 virtual disk imaged from a master target device delivers desktops and applications. This option is not available for cloud deployments.
- **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 virtual disk size in GB 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.
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.

**NIC (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.

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.

**Domain Credentials**

Click **Enter credentials** and enter user credentials with sufficient permissions to create machine accounts in Active Directory.

**Tip:**

The account you used to log into Studio is the same account you use to interact with Active Directory. When provisioning a new catalog, adding machines to a catalog, or removing a catalog and the machine names from Active Directory, a dialog appears requesting your Active Directory domain administrator credentials.
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

June 26, 2020

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.
- 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.
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 next shutdown will immediately affect any machines not currently in use, that is, machines that do not have an active user session. A system that is in use receives the update when the current active session ends. Consider the following:

- New sessions cannot be launched until the update has completed on applicable machines.
- For desktop OS machines, machines are immediately updated when the machine is not in use, or when users are not logged in.
- For a server OS with child machines, reboots do not occur automatically. They must be manually shut down and restarted.
Tip:
Limit the number of machines being rebooted by using the advanced settings for a host connection. Use these settings to modify the actions taken for a given catalog; advanced settings vary depending on the hypervisor.

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.
Citrix Virtual Apps and Desktops service

- 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.

Copied!
Failed!

Azure Quick Deploy

July 14, 2020

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.
Citrix Virtual Apps and Desktops service

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>Deploy to Azure</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Deploy to Amazon Web Services and Google Cloud</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Deploy to on-premises hypervisors</td>
<td>No</td>
</tr>
<tr>
<td>Deliver</td>
<td>Deliver Windows apps</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Feature</th>
<th>Azure Quick Deploy</th>
<th>Full Configuration</th>
</tr>
</thead>
<tbody>
<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>Remote PC Access</td>
<td>No</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 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 resources, and then use the other method to create more 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 Virtual Apps and Desktops service

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 26, 2020

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:

• 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 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 delivery group being created, the console guides you to the correct selection (such as “Set up delivery groups 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 (multi-session OS, single-session 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) single-session OS machines. Choose either **Applications** or **Desktops**. You cannot enable both.

(If you selected machines from a multi-session OS or single-session 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 single-session OS machines, you can import user data (a list of users) later by editing the delivery group.)

Unauthenticated (anonymous): For delivery groups containing multi-session 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 multi-session OS VDA 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>
</tbody>
</table>
### Citrix Virtual Apps and Desktops service

<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>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.
Citrix Virtual Apps and Desktops service

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

Introduction

This article describes procedures for managing delivery groups from the management console. In addition to changing the settings specified when creating the group, you can configure other settings.
Citrix Virtual Apps and Desktops service

that are not available when you create a delivery group.

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 might 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 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 single-session 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

© 1999-2020 Citrix Systems, Inc. All rights reserved.
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 Autocore for information about proactively power managing machines.

Change assignments of machines to users in a delivery group

You can change the assignments of single-session OS machines provisioned with MCS. You cannot change assignments for multi-session 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 supersedes 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 multi-session 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 single-session 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 multi-session OS machine is in maintenance mode. Maintenance mode is on when any of the following occur:

- Maintenance mode is set to on, as described earlier.
- 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 might 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.
• **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 single-session 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 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 will likely 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 to restart all machines at the same time, or the total length of time to begin restarting all 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 the 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.

**Scheduled restarts delayed due to database outage**

*Note:*
This feature is available only in PowerShell.

If a site database outage occurs before a scheduled restart begins for machines (VDAs) in a delivery group, the restarts begin when the outage ends. This can have unintended results.

For example, let’s say you’ve scheduled a delivery group’s restarts to occur during off-production hours (beginning at 3 am). A site database outage occurs one hour before a scheduled restart begins (2 am). The outage lasts six hours (until 8 am). The restart schedule begins when the connection between the Delivery Controller and the site database is restored. The VDA restarts now begin five hours after their original schedule. This might result in VDAs restarting during production hours.

To help avoid this situation, you can use the **MaxOvertimeStartMins** parameter for the **New-BrokerRebootScheduleV2** and **Set-BrokerRebootScheduleV2** cmdlets. The value specifies the maximum number of minutes beyond the scheduled start time that a restart schedule can begin.

If the database connection is restored within that time (scheduled time + **MaxOvertimeStartMins**), the VDA restarts begin.

If the database connection is not restored within that time, the VDA restarts do not begin.

If this parameter is omitted, the scheduled restart begins when the connection to the database is restored, regardless of the outage duration.

For more information, see the cmdlet help. This feature is available only in PowerShell.

**Scheduled restarts for machines in maintenance mode**

*Note:*
This feature is available only in PowerShell.

To indicate whether a restart schedule affects machines that are in maintenance mode, use the **IgnoreMaintenanceMode** option with **BrokerRebootScheduleV2** cmdlets.

For example, the following cmdlet creates a schedule that restarts machines that are in maintenance mode (in addition to machines that are not in maintenance mode).

```powershell
New-BrokerRebootSchedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

The following cmdlet modifies an existing restart schedule.
The command to set the reboot schedule with maintenance mode ignored is:

```
Set-BrokerRebootSchedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

For more information, see the cmdlet help. This feature is available only in PowerShell.

**Load manage machines in delivery groups**

You can load manage multi-session 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 multi-session OS machine is considered for load balancing only when maintenance mode is off.

- **Server load index**: Determines how likely a server delivering multi-session 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.

- **Horizontal or vertical load balancing**: Horizontal and vertical load balancing are site-wide settings. By default, horizontal load balancing is enabled. Horizontal load balancing assigns the incoming load to the least-loaded RDS machine. Although horizontal load balancing offers high user performance, it can increase costs as more machines are kept powered-on and busy.

  As an alternative, you can use PowerShell to enable vertical load balancing. Vertical load balancing assigns the incoming load to the most-loaded RDS machine that has not reached a high watermark. This saturates existing machines before moving on to new machines. As users disconnect and free up capacity on existing machines, new load is assigned to those machines.
To enable or disable vertical load balancing site-wide, use the `UseVerticalScalingForRdsLaunches` setting in the `Set-BrokerSite` cmdlet. Display the setting’s value with `Get-BrokerSite`. See the cmdlet help for details.

**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 multi-session OS machines.

The session prelaunch and session linger features help specified users access applications quickly, by:

- Starting sessions before they are requested (session prelaunch)
- 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 multi-session OS, minimum version 7.6.
- These features are supported only when using Citrix Workspace app for Windows, and also require more 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 application availability for users against the cost of keeping licenses in use and resources allocated.

• You can also configure session prelaunch for a scheduled time of day in 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.
Citrix Virtual Apps and Desktops service

- 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**

June 26, 2020
**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 subdividing (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 machine 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 balanced. 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 (Calculator 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 upgrading your delivery groups 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.

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 group creation 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 group creation 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**.

**Copied!**

**Failed!**

### Manage application groups

August 18, 2020

**Introduction**

This article describes how to manage the application groups you **created**.
See **Applications** for information about managing applications in application groups or delivery groups, including how to:

- Add or remove applications in an application group.
- Change application group associations.

Managing application groups requires the delegated administration permissions of the Delivery Group Administrator built-in role. For details, see **Delegated administration**.

**Enable or disable an application group**

When an application group is enabled, it can deliver the applications that have been added to it. Disabling an application group disables each application in that group. However, if those applications are also associated with other enabled application groups, they can be delivered from those other groups. Similarly, if the application was explicitly added to delivery groups associated with the application group (in addition to being added to the application group), disabling the application group does not affect the applications in those delivery groups.

An application group is enabled when you create it. You cannot change this when you create the group.

1. Select **Applications** in the Studio navigation pane.
2. Select an application group in the middle pane and then select **Edit Application Group** in the Actions pane.
3. On the **Settings** page, select or clear the **Enable Application Group** check box.
4. Click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

**Enable or disable application session sharing between application groups**

Session sharing between application groups is enabled when you create an application group. You cannot change this when you create the group. For more information, see **Session sharing with application groups**.

1. Select **Applications** in the Studio navigation pane.
2. Select an application group in the middle pane and then select **Edit Application Group** in the Actions pane.
3. On the **Settings** page, select or clear the **Enable application session sharing between Application Groups** check box.
4. Click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.
Disable application session sharing within an application group

Session sharing between applications in the same application group is enabled by default when you create an application group. If you disable application session sharing between application groups, session sharing between applications in the same application group remains enabled.

You can use the PowerShell SDK to configure application groups with application session sharing disabled between the applications they contain. In some circumstances this may be desirable. For example, you might want users to start non-seamless applications in full-size application windows on separate monitors.

When you disable application session sharing within an application group, each application in that group launches in a new application session. If a suitable disconnected session is available which is running the same application, it is reconnected. For example, if you launch Notepad, and there is a disconnected session with Notepad running, that session is reconnected instead of creating a new one. If multiple suitable disconnected sessions are available, one of the sessions is chosen to reconnect to, in a random but deterministic manner. If the situation reoccurs in the same circumstances, the same session is chosen, but the session is not necessarily predictable otherwise.

You can use the PowerShell SDK either to disable application session sharing for all applications in an existing application group, or to create an application group with application session sharing disabled.

PowerShell cmdlet examples

To disable session sharing, use the Broker PowerShell cmdlets New-BrokerApplicationGroup or Set-BrokerApplicationGroup with the parameter SessionSharingEnabled set to False and the parameter SingleAppPerSession set to True.

- For example, to create an application group with application session sharing disabled for all applications in the group:

  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True

- For example, to disable application session sharing between all applications in an existing application group:

  Set-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
Considerations

• To enable the SingleAppPerSession property you must set the SessionSharingEnabled property to False. The two properties must not be enabled at the same time. The SessionSharingEnabled parameter refers to sharing sessions between application groups.

• Application session sharing works only for applications that are associated with application groups but are not associated with delivery groups. All applications associated directly with a delivery group share sessions by default.

• If an application is assigned to multiple application groups, make sure that the groups do not have conflicting settings. For example, one group with the option set to True, and another group’s option set to False results in unpredictable behavior.

Rename an application group

1. Select Applications in the Studio navigation pane.
2. Select an application group in the middle pane and then select Rename Application Group in the Actions pane.
3. Specify the new unique name and then click OK.

Add, remove, or change the priority of delivery group associations with an application group

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 version earlier than 7.9.
• You have Edit Delivery Group permission.

The delivery group type is automatically converted to “desktops and applications” when the Edit Application Group dialog is committed.

1. Select Applications in the Studio navigation pane.
2. Select an application group in the middle pane and then select Edit Application Group in the Actions pane.
3. Select the Delivery Groups page.
4. To add delivery groups, click Add. Select the check boxes of available delivery groups. (Incompatible delivery groups cannot be selected.) When you finish your selections, click OK.
5. To remove delivery groups, select the check boxes of the groups you want to remove and then click **Remove**. Confirm the deletion when prompted.
6. To change the priority of delivery groups, select the checkbox of the delivery group and then click **Edit Priority**. Enter the priority (0 = highest) and then click **OK**.
7. Click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

### Add, change, or remove a tag restriction in an application group

Adding, changing, and removing tag restrictions can have unanticipated effects on which machines are considered for application launch. Review the considerations and cautions in **Tags**.

1. Select **Applications** in the Studio navigation pane.
2. Select an application group in the middle pane and then select **Edit Application Group** in the Actions pane.
3. Select the **Delivery Groups** page.
4. To add a tag restriction, select **Restrict launches to machines with the tag** and then select the tag from the dropdown.
5. To change or remove a tag restriction, either select a different tag from the dropdown or remove the tag restriction entirely 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.

### Add or remove users in an application group

For detailed information about users, see **Create application groups**.

1. Select **Applications** in the Studio navigation pane.
2. Select an application group in the middle pane and then select **Edit Application Group** in the Actions pane.
3. Select the **Users** page. Indicate whether you want to allow all users in the associated delivery groups to use applications in the application group, or only specific users and groups. 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**.
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 scopes in an application group

You can change a scope only if you have created a scope (you cannot edit the All scope). For more information, see Delegated administration.

1. Select Applications in the Studio navigation pane.
2. Select an application group in the middle pane and then select Edit Application Group in the Actions pane.
3. Select the Scopes page. Select or clear the check box next to a scope.
4. Click Apply to apply any changes you made and keep the window open, or click OK to apply changes and close the window.

Delete an application group

An application must be associated with at least one delivery group or application group. If deleting an application group will result in one or more applications no longer belonging to a group, you will be warned that deleting that group will also delete those applications. You can then confirm or cancel the deletion.

Deleting an application does not delete it from its original source. However, if you want to make it available again, you must add it again.

1. Select Applications in the Studio navigation pane.
2. Select an application group in the middle pane and then select Delete Group in the Actions pane.
3. Confirm the deletion when prompted.

Remote PC Access

August 11, 2020

Remote PC Access is a feature of Citrix Virtual Apps and Desktops that enables organizations to easily allow their employees to access corporate resources remotely in a secure manner. The Citrix platform makes this secure access possible by giving users access to their physical office PCs. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Remote PC Access eliminates the need to introduce and provide other tools to accommodate teleworking. For example, virtual desktops or applications and their associated infrastructure.
Citrix Virtual Apps and Desktops service

Remote PC Access uses the same Citrix Virtual Apps and Desktops components that deliver virtual desktops and applications. As a result, the requirements and process of deploying and configuring Remote PC Access are the same as those required for deploying Citrix Virtual Apps and Desktops for the delivery of virtual resources. This uniformity provides a consistent and unified administrative experience. Users receive the best user experience by using Citrix HDX to deliver their office PC session.

The feature consists of a machine catalog of type **Remote PC Access** that provides this functionality:

- Ability to add machines by specifying OUs. This ability facilitates the addition of PCs in bulk.
- Automatic user assignment based on the user that logs into the office Windows PC. We support single user and multiple users assignments.

Citrix Virtual Apps and Desktops can accommodate more use cases for physical PCs by using other types of machine catalogs. These use cases include:

- Physical Linux PCs
- Pooled physical PCs (that is, randomly assigned, not dedicated)

**Notes:**

For details on the supported OS versions, see the system requirements for the VDA for **single-session OS** and **Linux VDA**.

For on-premises deployments, Remote PC Access is valid only for Citrix Virtual Apps and Desktops Advanced or Premium licenses. Sessions consume licenses in the same way as other Citrix Virtual Desktops sessions. For Citrix Cloud, Remote PC Access is valid for the Citrix Virtual Apps and Desktops Service and Workspace Premium Plus.

**Considerations**

While all the technical requirements and considerations that apply to Citrix Virtual Apps and Desktops in general also apply to Remote PC Access, some might be more relevant or exclusive to the physical PC use case.

**Deployment considerations**

While planning the deployment of Remote PC Access, make a few general decisions.

- You can add Remote PC Access to an existing Citrix Virtual Apps and Desktops deployment. Before choosing this option, consider the following:
  - Are the current Delivery Controllers or Cloud Connectors appropriately sized to support the additional load associated with the Remote PC Access VDAs?
  - Are the on-premises site databases and database servers appropriately sized to support the additional load associated with the Remote PC Access VDAs?
Citrix Virtual Apps and Desktops service

- Will the existing VDAs and the new Remote PC Access VDAs exceed the number of maximum supported VDAs per site?
- You must deploy the VDA to office PCs through an automated process. The following are two of options available:
  - Electronic Software Distribution (ESD) tools such as SCCM: Install VDAs using SCCM.
  - Deployment scripts: Install VDAs using scripts.
- Review the Remote PC Access security considerations.

Machine catalog considerations

The type of machine catalog required depends on the use case:

- Remote PC Access
  - Windows dedicated PCs
  - Windows dedicated multi-user PCs
- Single-session OS
  - Static - Dedicated Linux PCs
  - Random - Pooled Windows and Linux PCs

Once you identify the type of machine catalog, consider the following:

- A machine can be assigned to only one machine catalog at a time.
- To facilitate delegated administration, consider creating machine catalogs based on geographic location, department, or any other grouping that eases delegating administration of each catalog to the appropriate administrators.
- When choosing the OUs in which the machine accounts reside, select lower-level OUs for greater granularity. If such granularity is not required, you can choose higher-level OUs. For example, in the case of Bank/Officers/Tellers, select Tellers for greater granularity. Otherwise, you can select Officers or Bank based on the requirement.
- Moving or deleting OUs after being assigned to a Remote PC Access machine catalog affects VDA associations and causes issues with future assignments. Therefore, make sure to plan accordingly so that OU assignment updates for machine catalogs are accounted for in the Active Directory change plan.
- If it is not easy to choose OUs to add machines to the machine catalog because of the OU structure, you don’t have to select any OUs. You can use PowerShell to add machines to the catalog afterward. User auto-assignments continue to work if the desktop assignment is configured correctly in the delivery group. A sample script to add machines to the machine catalog along with user assignments is available in GitHub.
- Integrated Wake on LAN is available only with the Remote PC Access type machine catalog.
Linux VDA considerations

These considerations are specific to the Linux VDA:

- Use the Linux VDA on physical machines only in non-3D mode. Due to limitations on NVIDIA’s driver, the local screen of the PC cannot be blacked out and displays the activities of the session when HDX 3D mode is enabled. Showing this screen is a security risk.
- Use machine catalogs of type single-session OS for physical Linux machines.
- The integrated Wake on LAN functionality is not available for Linux machines.

Technical requirements and considerations

This section contains the technical requirements and considerations for physical PCs.

- The following are not supported:
  - KVM switches or other components that can disconnect a session.
  - Hybrid PCs, including All-in-One and NVIDIA Optimus laptops and PCs.
- Connect the keyboard and mouse directly to the PC. Connecting to the monitor or other components that can be turned off or disconnected, can make these peripherals unavailable. If you must connect the input devices to components such as monitors, do not turn those components off.
- The PCs must be joined to an Active Directory Domain Services domain.
- Secure Boot is supported on Windows 10 only.
- The PC must have an active network connection. A wired connection is preferred for greater reliability and bandwidth.
- If using Wi-Fi, do the following:
  1. Set the power settings to leave the wireless adapter turned on.
  2. Configure the wireless adapter and network profile to allow automatic connection to the wireless network before the user logs on. Otherwise, the VDA does not register until the user logs on. The PC isn’t available for remote access until a user has logged on.
  3. Ensure that the Delivery Controllers or Cloud Connectors can be reached from the Wi-Fi network.
- You can use Remote PC Access on laptop computers. Ensure the laptop is connected to a power source instead of running on the battery. Configure the laptop power options to match the options of a desktop PC. For example:
  1. Disable the hibernate feature.
  2. Disable the sleep feature.
  3. Set the close lid action to Do Nothing.
4. Set the “press the power button” action to **Shut Down**.
5. Disable video card and NIC energy-saving features.

- Remote PC Access is supported on Surface Pro devices with Windows 10. Follow the same guidelines for laptops mentioned previously.

- If using a docking station, you can undock and redock laptops. When you undock the laptop, the VDA reregisters with the Delivery Controllers or Cloud Connectors over Wi-Fi. However, when you redock the laptop, the VDA doesn’t switch to use the wired connection unless you disconnect the wireless adapter. Some devices provide built-in functionality to disconnect the wireless adapter upon establishing a wired connection. The other devices require custom solutions or third-party utilities to disconnect the wireless adapter. Review the Wi-Fi considerations mentioned previously.

Do the following to enable docking and undocking for Remote PC Access devices:

1. In the **Start** menu, select **Settings > System > Power & Sleep**, and set **Sleep** to **Never**.
2. Under the **Device Manager > Network adapters > Ethernet adapter** go to **Power Management** and clear **Allow the computer to turn off this device to save power**. Ensure that **Allow this device to wake the computer** is checked.

- Multiple users with access to the same office PC see the same icon in Citrix Workspace. When a user logs on to Citrix Workspace, that resource appears as unavailable if already in use by another user.

- Install the Citrix Workspace app on each client device (for example, a home PC) that accesses the office PC.

**Configuration sequence**

This section contains an overview of how to configure Remote PC Access when using the **Remote PC Access** type machine catalog. For information on how to create other types of machine catalogs, see the [Create machine catalogs](#).

1. On-premises site only - To use the integrated Wake on LAN feature, configure the prerequisites outlined in [Wake on LAN](#).

2. If a new Citrix Virtual Apps and Desktops site was created for Remote PC Access:
   a) Select the **Remote PC Access** site type.
   b) On the **Power Management** page, choose to enable or disable power management for the default Remote PC Access machine catalog. You can change this setting later by editing the machine catalog properties. For details on configuring Wake on LAN, see [Wake on LAN](#).
   c) Complete the information on the **Users** and **Machine Accounts** pages.
Completing these steps creates a machine catalog named **Remote PC Access Machines** and a delivery group named **Remote PC Access Desktops**.

3. If adding to an existing Citrix Virtual Apps and Desktops site:
   
a) Create a machine catalog of type **Remote PC Access** (Operating System page of the wizard). For details on how to create a machine catalog, see [Create machine catalogs](#). Make sure to assign the correct OU so that the target PCs are made available for use with Remote PC Access.

   b) Create a delivery group to provide users access to the PCs in the machine catalog. For details on how to create a delivery group, see [Create delivery groups](#). Make sure to assign the delivery group to an Active Directory group that contains the users that require access to their PCs.

4. Deploy the VDA to the office PCs.
   
   - We recommend using the single-session OS core VDA installer (VDAWorkstationCore-Setup.exe).
   
   - You can also use the single-session full VDA installer (VDAWorkstationSetup.exe) with the `/remotecp` option, which achieves the same outcome as using the core VDA installer.
   
   - Consider enabling Windows Remote Assistance to allow help desk teams to provide remote support through Citrix Director. To do so, use the `/enable_remote_assistance` option. For details, see [Install using the command line](#).

   - To be able to see logon duration information in Director, you must use the single-session full VDA installer and include the **Citrix User Profile Manager WMI Plugin** component. Include this component by using the `/includeadditional` option. For details, see [Install using the command line](#).

   - For information about deploying the VDA using SCCM, see [Install VDAs using SCCM](#).

   - For information about deploying the VDA through deployment scripts, see [Install VDAs using scripts](#).

After you successfully complete steps 2–4, users are automatically assigned to their own machines when they log in locally on the PCs.

5. Instruct users to download and install Citrix Workspace app on each client device that they use to access the office PC remotely. Citrix Workspace app is available from [https://www.citrix.com/downloads/](https://www.citrix.com/downloads/) or the application stores for supported mobile devices.

### Features managed through the registry

**Caution:**

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.

**Disable multiple user auto-assignments**

On each Delivery Controller, add the following registry setting:

HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer
  - Name: AllowMultipleRemotePCAssignments
  - Type: DWORD
  - Data: 0

**Sleep mode (minimum version 7.16)**

To allow a Remote PC Access machine to go into a sleep state, add this registry setting on the VDA, and then restart the machine. After the restart, the operating system power saving settings are respected. The machine goes into sleep mode after the preconfigured idle timer passes. After the machine wakes up, it reregisters with the Delivery Controller.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA
  - Name: DisableRemotePCSleepPreventer
  - Type: DWORD
  - Data: 1

**Session management**

By default, a remote user's session is automatically disconnected when a local user initiates a session on that machine (by pressing CTRL+ALT+DEL). To prevent this automatic action, add the following registry entry on the office PC, and then restart the machine.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC
  - Name: SasNotification
  - Type: DWORD
  - Data: 1

By default, the remote user has preference over the local user when the connection message is not acknowledged within the timeout period. To configure the behavior, use this setting:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC
  - Name: RpcaMode
  - Type: DWORD
Citrix Virtual Apps and Desktops service

- Data:
  - 1 - The remote user always has preference if he or she does not respond to the messaging UI in the specified timeout period. This behavior is the default if this setting is not configured.
  - 2 - The local user has preference.

The timeout for enforcing the Remote PC Access mode is 30 seconds by default. You can configure this timeout but do not set it lower than 30 seconds. To configure the timeout, use this registry setting:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`
- Name: RpcaTimeout
- Type: DWORD
- Data: number of seconds for timeout in decimal values

When a user wants to forcibly get the console access: The local user can press Ctrl+Alt+Del twice in a gap of 10 seconds to get local control over a remote session and force a disconnect event.

After the registry change and machine restart, if a local user presses Ctrl+Alt+Del to log on to that PC while it is in use by a remote user, the remote user receives a prompt. The prompt asks whether to allow or deny the local user’s connection. Allowing the connection disconnects the remote user’s session.

### Wake on LAN

Integrated Wake on LAN is available only in on-premises Citrix Virtual Apps and Desktops and requires Microsoft System Center Configuration Manager (SCCM).

Remote PC Access supports Wake on LAN, which gives users the ability to turn on physical PCs remotely. This feature enables users to keep their office PCs turned off when not in use, saving energy costs. It also enables remote access when a machine has been turned off inadvertently. For example, because of a power outage.

The Remote PC Access Wake on LAN feature is supported with PCs that have the Wake on LAN option enabled in the BIOS/UEFI.

### SCCM and Remote PC Access Wake on LAN

To configure the Remote PC Access Wake on LAN feature, complete the following before deploying the VDA:

- Configure SCCM 2012 R2, 2016, or 2019 within the organization. Then deploy the SCCM client to all Remote PC Access machines, allowing time for the scheduled SCCM inventory cycle to run (or force one manually, if necessary).
- For SCCM Wake Proxy or magic packet support:
Citrix Virtual Apps and Desktops service

- Configure Wake on LAN in each PC’s BIOS/UEFI settings.
- For Wake Proxy support, enable the option in SCCM. For each subnet in the organization that contains PCs that use the Remote PC Access Wake on LAN feature, ensure that three or more machines can serve as sentinel machines.
- For magic packet support, configure network routers and firewalls to allow magic packets to be sent, using either a subnet-directed broadcast or unicast.

After you install the VDA on office PCs, enable or disable power management when you create the connection and the machine catalog.

- If you enable power management in the catalog, specify connection details: the SCCM address, access credentials, and connection name. The access credentials must have access to collections in the scope and the Remote Tools Operator role.
- If you do not enable power management, you can add a power management (Configuration Manager) connection later and then edit a Remote PC Access machine catalog to enable power management.

You can edit a power management connection to configure advanced settings. You can enable:

- Wake-up proxy delivered by SCCM.
- Wake on LAN (magic) packets. If you enable Wake on LAN packets, you can select a Wake on LAN transmission method: subnet-directed broadcasts or Unicast.

The PC uses AMT power commands (if they are supported), plus any of the enabled advanced settings. If the PC does not use AMT power commands, it uses the advanced settings.

Troubleshoot

Monitor blanking not working

If the Windows PC’s local monitor is not blank while there is an active HDX session (the local monitor displays what’s happening in the session) it is likely due to issues with the GPU vendor’s driver. To resolve the issue, give the Citrix Indirect Display driver (IDD) higher priority than the graphic card’s vendor driver by setting the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits
```

- Name: CitrixIDD
- Type: DWORD
- Data: 3

For more details about display adapter priorities and monitor creation, see the Knowledge Center article CTX237608.
**Session disconnects when you select Ctrl+Alt+Del on the machine that has session management notification enabled**

The session management notification controlled by the SasNotification registry value only works when Remote PC Access mode is enabled on the VDA. If the physical PC has the Hyper-V role or any virtualization-based security features enabled, the PC reports as a virtual machine. If the VDA detects that it is running on a virtual machine, it automatically disables Remote PC Access mode. To enable Remote PC Access mode, add the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA
```

- **Name:** ForceEnableRemotePC
- **Type:** DWORD
- **Data:** 1

Restart the PC for the setting to take effect.

**Diagnostic information**

Diagnostic information about Remote PC Access is written to the Windows Application Event log. Informational messages are not throttled. Error messages are throttled by discarding duplicate messages.

- 3300 (informational): Machine added to catalog
- 3301 (informational): Machine added to delivery group
- 3302 (informational): Machine assigned to user
- 3303 (error): Exception

**Power management**

If power management for Remote PC Access is enabled, subnet-directed broadcasts might fail to start machines that are on a different subnet from the Controller. If you need power management across subnets using subnet-directed broadcasts, and AMT support is not available, try the Wake-up proxy or Unicast method. Ensure those settings are enabled in the advanced properties for the power management connection.

**The active remote session records the local touchscreen input**

When the VDA enables Remote PC Access mode, the machine ignores the local touchscreen input during an active session. If the physical PC has the Hyper-V role or any virtualization-based security features enabled, the PC reports as a virtual machine. If the VDA detects that it is running on a virtual machine, it automatically disables Remote PC Access mode. To enable Remote PC Access mode, add the following registry setting:
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

- Name: ForceEnableRemotePC
- Type: DWORD
- Data: 1

Restart the PC for the setting to take effect.

More resources

The following are other resources for Remote PC Access:


Remove components

April 9, 2020

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 multi-session 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 single-session OS machine.

VDAWorkstationSetup.exe /remove /components vda

You can also remove a VDA using a script provided by Citrix. See Remove VDAs using the script.

User personalization layer

June 22, 2020

The user personalization layer feature for Citrix Virtual Apps and Desktops extends the capabilities of non-persistent machine catalogs. User personalization layers preserve users’ data and locally installed applications across sessions. Powered by Citrix App Layering, this feature replaces Personal vDisk (PvD).

Like PvD, the user personalization layer feature supports Citrix Provisioning and Machine Creation Services (MCS) in a non-persistent machine catalog. You install the feature components alongside the Virtual Delivery Agent within the master image.

A VHD file stores any applications that the user installs locally. The VHD, which is mounted on the image, acts as the user's own user layer virtual hard drive.

This document includes instructions for deploying and configuring the user personalization layer feature. It describes the requirements for successful deployment, limitations, and known issues.

To use the User personalization layer feature, you must first deploy it using the steps detailed in the article. Until then, the feature is not available for you to use.
Application support

Aside from the following exceptions, all applications that a user installs locally on the desktop are supported in the user personalization layer.

Exceptions

The following applications are the exception and are not supported on the user personalization layer:

- Enterprise applications, such as MS Office and Visual Studio.
- Applications that modify the network stack or hardware. Example: a VPN client.
- Applications that have boot level drivers. Example: a virus scanner.
- Applications with drivers that use the driver store. Example: a printer driver.

Note:
You can make printers available using Windows Group Policy Objects (GPOs).

Do not allow users to install any unsupported applications locally. Rather, install these applications directly on the master image.

Applications that require a local user or administrator account

When a user installs an application locally, the app goes into their user layer. If the user then adds or edits a local user or group, the changes do not persist beyond the session.

Important:
Add any required local user or group in the master image.

Requirements

The user personalization layer feature requires the following components:

- Citrix Virtual Apps and Desktops 7.1909 or later
- Virtual Delivery Agent (VDA), version 1912
- Citrix Provisioning, version 1909 or later
- Windows File Share (Server Message Block protocol, SMB)

You can deploy the User personalization layer feature on the following Windows versions when the OS is deployed as single session. Support is limited to a single user on a single session.

- Windows 10 Enterprise x64, version 1607 or later
Citrix Virtual Apps and Desktops service

- Windows 10 Multi-Session*
- Windows Server 2016*
- Windows Server 2019*

*For Citrix Virtual Apps and Desktops 7, Azure Files with User personalization layers is supported on Windows Server 2019, Windows Server 2016v and Windows 10 client. User personalization layer is only supported as a Server VDI deployment. For deployment details, see the Server VDI article.

If you installed the preview version of the user personalization layer feature, uninstall the software and reboot the master image before installing this release.

**Set up your file share**

The user personalization layer feature requires Windows Server Message Block (SMB) storage. To create a Windows file share, follow the usual steps for the Windows operating system that you are on.

For details about using Azure Files with Azure-based catalogs, see Set up Azure Files storage for User personalization layers.

**Recommendations**

Follow the recommendations in this section for a successful user personalization layer deployment.

**Profile Management solution**

User personalization layer stores all changes the user makes for a single machine catalog image. To add enhanced capabilities such as roaming profile data across multiple catalog images, Citrix recommends also using Profile Management. Refer to the Profile Management documentation for more details.

When using Profile Management with the user personalization layer feature, clear deletion of the user's information on logoff. You can clear deletion using a Group Policy Object (GPO) or the policy on the Delivery Controller (DDC).

For details about available Profile Management policies, see Profile Management policy descriptions and defaults.

**Microsoft System Center Configuration Manager (SCCM)**

If you are using SCCM with the user personalization layer feature, follow the Microsoft guidelines for preparing your image in a VDI environment. Refer to this Microsoft TechNet article for more information.
**Maximum user layer size**

We recommend at least 10 GB as the user layer size.

*Note:*

During installation, the value zero (0) results in the default user layer size of 10 GB.

**A quota set in Windows can override the maximum user layer size**

You can override Studio's maximum user layer size by defining a quota for the user layer file share. The user layer size is set to a maximum of the quota size.

To set a hard quota on the user layer size, use either of Microsoft's quota tools:

- File Server Resource Manager (FSRM)
- Quota Manager

The quota must be set on the user layer directory named Users.

*Note:*

Increasing or decreasing the quota only impacts new user layers. It does not change the maximum size of existing user layers. Existing user layers remain unchanged when the quota is updated.

**Deploy a User personalization layer**

When deploying the user personalization feature, you define the policies within Studio. You then assign the policies to the delivery group bound to the machine catalog, where the feature is deployed.

If you leave the master image with no user personalization layer configuration, the services remain idle and do not interfere with authoring activities.

If you set the policies in the master image, the services attempt to run and mount a user layer within the master image. The master image would exhibit unexpected behaviors and instability.

To deploy the user personalization layer feature, complete the following steps in this order:

- Step 1: Verify availability of a Citrix Virtual Apps and Desktops environment.
- Step 2: Prepare your master image.
- Step 3: Create a machine catalog.
- Step 4: Create a delivery group.
- Step 5: Create delivery group custom policies.
Step 1: Verify that the Citrix Virtual Apps and Desktops environment is available

Be sure that your Citrix Virtual Apps and Desktops environment is available to use with this new feature. For setup details, see Install and configure Citrix Virtual Apps and Desktops.

Step 2: Prepare your master image

To prepare your master image:

1. Locate the master image. Install your organization’s enterprise applications and any other apps your users generally find useful.

2. If you are deploying Server VDI, follow the steps in the Server VDI article. Be sure to include the optional component, User personalization layer. For details, see the Command-line options to install a VDA.

3. If you are using Windows 10, install Virtual Delivery Agent (VDA) 1912. If an older version of the VDA is already installed, uninstall the old version first. When installing the new version, be sure to select and install the optional component, Citrix User Personalization Layer, as follows:

   a) Click the tile, Virtual Delivery Agent for Windows Desktop OS:
a) **Environment:** Select either Create a master MCS image or Create a master image using Citrix Provisioning or third-party provisioning tools.

![Image of Citrix Virtual Apps and Desktops 7 configuration screen]

a) **Core Components:** Click *Next*.

b) **Additional Components:** Check *Citrix User Personalization Layer*. 
a) Click through the remaining installation screens, configuring the VDA as needed, and click Install. The image reboots one or more times during installation.

4. Leave Windows updates disabled. The user personalization layer installer disables Windows updates on the image. Leave the updates disabled.

The image is ready for you to upload into Studio.

**Step 3: Create a machine catalog**

In Studio, follow the steps to create a machine catalog. Use the following options during catalog creation:

1. Select *Operating System* and set it to *Single session OS*.

2. Select *Machine Management* and set it to *Machines that are power managed*. For example, virtual machines or blade PCs.

3. Select *Desktop Experience* and set it to either *pooled-random* or *pooled-static* catalog type, as in the following examples:
   
   • *Pooled-random:*
• **Pooled-static**: If you select pooled-static, configure desktops to discard all changes and clear virtual desktops when the user logs off, as shown in the following screenshot:
Step 4: Create a delivery group

Create and configure a delivery group, including machines from the machine catalog you created. For details, see the Create Delivery Groups.

Step 5: Create delivery group custom policies

To enable mounting of user layers within the Virtual Delivery Agents, you use configuration parameters to specify:

- Where on the network to access the user layers.
- How large to permit the user layer disks to grow.
To define the parameters as custom Citrix policies in Studio and assign them to your delivery group.

1. In Studio, select Policies in the navigation pane:

2. Select Create Policy in the Actions pane. The Create Policy window appears.

3. Type ‘user layer’ into the search field. The following two policies appear in the list of available policies:
   - User Layer Repository Path
   - User Layer Size GB

   **Note:**
   Changing the User Layer Size in the policy does not change the size of existing layers.

4. Click **Select** next to User Layer Repository Path. The Edit Setting window appears.
5. Enter a path in the format `\\server name or address\folder name` in the Value field, then click OK:
6. Optional: Click **Select** next to User Layer Size in GB:
7. The Edit Settings window appears.

8. Optional: Change the default value of ‘0’ to the maximum size (in GB) that the user layer can grow. Click OK.

   **Note:**
   If you keep the default value, the maximum user layer size is 10 GB.

9. Click Next to configure Users and Machines. Click the Delivery Group Assign link highlighted in this image:
10. In the Delivery Group menu, select the delivery group created in the previous section. Click OK.
11. Enter a name for the policy. Click the check box to enable the policy, and click Finish.
**Configure security settings on the user layer folder**

As a domain administrator, you can specify more than one storage location for your user layers. Create a `\Users` subfolder for each storage location (including the default location). Secure each location using the following settings.

<table>
<thead>
<tr>
<th>Setting name</th>
<th>Value</th>
<th>Apply to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creator Owner</td>
<td>Modify</td>
<td>Subfolders and Files only</td>
</tr>
<tr>
<td>Owner Rights</td>
<td>Modify</td>
<td>Subfolders and Files only</td>
</tr>
<tr>
<td>Users or group:</td>
<td>Create Folder, Append Data, Traverse Folder, Execute File, List Folders, Read Data, Read Attributes</td>
<td>Selected Folder Only</td>
</tr>
<tr>
<td>System</td>
<td>Full Control</td>
<td>Selected Folder, Subfolders, and Files</td>
</tr>
</tbody>
</table>
### User layer messages

When a user is unable to access their user layer, they receive one of these notification messages.

- **User Layer In Use**
  
  We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.

- **User Layer Unavailable**

  We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.

- **System not reset after user sign-out**

  This system was not shut down properly. Please log off immediately and contact your system administrator.

### Log files to use when troubleshooting

The log file, ulayersvc.log, contains the output of the user personalization layer software where changes are logged.

```bash
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

### Limitations

Keep the following limitations in mind when installing and using the user personalization layer feature.

- Do not configure the user personalization layer feature with persistent machine catalogs.
- Do not use Session hosts.
• Do not update the machine catalog with an image running a new OS install (even the same version of Windows 10). Best practice is to apply updates to the OS within the same master image used when creating the machine catalog.

• Do not use boot-time drivers, nor any other early boot personalization.

• Do not migrate PVD data to the user personalization layer feature.

• Do not migrate existing user layers from the full App Layering product to the user personalization layer feature.

• Do not change the user layer SMB path to access user layers created using a different master OS image.

• Do not enable Secure Boot within User personalization layer virtual machines, as it is not currently supported.

• When a user logs out of a session and then logs in again, the new session runs on a different machine in the pool. In a VDI environment, Microsoft Software Center lists an application as **Installed** on the first machine, but shows it as **Unavailable** on the second machine.

  To find out the true status of the application, instruct the user to select the application in Software Center and click **Install**. SCCM then updates the status to the true value.

• Software Center occasionally stops immediately after launching within a VDA that has the user personalization layer feature enabled. To avoid this issue, follow Microsoft’s recommendations for **Implementing SCCM in a XenDesktop VDI environment**. Also, make sure that the `ccmexec` service is running before you start the Software Center.

• In Group Polices (Computer Settings), User layer settings override settings applied to the master image. Therefore, changes you make in Computer Settings using a GPO are not always present for the user on the next session login.

  To get around this issue, create a User Logon Script that issues the command:

  ```
gpupdate /force
  ```

  For example, one customer set the following command to run at each user login:

  ```
gpupdate /Target:Computer /force
  ```

  For best results, apply changes to Computer Settings directly on the user layer, after the user has logged in.
Upgrade

January 15, 2020

Important notice about upgrading VDAs

If the Personal vDisk (PvD) component was ever installed on a VDA, that VDA cannot be upgraded to version 1912 LTSR or later. To use the new VDA, you must uninstall the current VDA and then install the new VDA.

This instruction applies even if you never used PvD.

Learn if you’re affected

How PvD might have been installed in earlier versions:

- In the VDA installer’s graphical interface, PvD was an option on the Additional Components page. The 7.15 LTSR and earlier 7.x releases enabled this option by default. So, if you accepted the defaults (or explicitly enabled the option in any release), PvD was installed.
- On the command line, the /baseimage option installed PvD. If you specified this option, or used a script that contained this option, PvD was installed.

If you don’t know whether your VDA has PvD installed, run the installer for the new VDA (1912 LTSR or later) on the machine or image.

- If PvD is installed, a message appears, indicating there is an incompatible component.
  - For the graphical interface, click Cancel on the page containing the message, and then confirm that you want to close the installer.
  - From the CLI, the command simply fails with the displayed message.
- If PvD is not installed, the upgrade proceeds.

What to do

If the VDA does not have PvD installed, follow the usual upgrade procedure.

If the VDA has PvD installed:

1. Uninstall the current VDA. For details, see Remove components.
2. Install the new VDA.

If you want to continue using PvD on your Windows 7 or Windows 10 (1607 and earlier, without updates) machines, VDA 7.15 LTSR is the latest supported version.
Introduction

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
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
- 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.

Copied!

Failed!

**HDX**

August 21, 2020

**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.

Citrix HDX delivers a high-definition experience to users of centralized applications and desktops, on any device and over any network.

HDX is designed around three technical principles:

- Intelligent redirection
- Adaptive compression
- Data de-duplication
Applied in different combinations, they optimize the IT and user experience, decrease bandwidth consumption, and increase user density per hosting server.

- **Intelligent redirection** - Intelligent redirection examines screen activity, application commands, endpoint device, and network and server capabilities to instantly determine how and where to render an application or desktop activity. Rendering can occur on either the endpoint device or hosting server.

- **Adaptive compression** - Adaptive compression allows rich multimedia displays to be delivered on thin network connections. HDX first evaluates several variables, such as the type of input, device, and display (text, video, voice, and multimedia). It chooses the optimal compression codec and the best proportion of CPU and GPU usage. It then intelligently adapts based on each unique user and basis. This intelligent adaptation is per user, or even per session.

- **Data de-duplication** - De-duplication of network traffic reduces the aggregate data sent between client and server. It does so by taking advantage of repeated patterns in commonly accessed data such as bitmap graphics, documents, print jobs, and streamed media. Caching these patterns allows only the changes to be transmitted across the network, eliminating duplicate traffic. HDX also supports multicasting of multimedia streams, where a single transmission from the source is viewed by multiple subscribers at one location, rather than a one-to-one connection for each user.

For more information, see *Boost productivity with a high-definition user workspace.*
Citrix Virtual Apps and Desktops service

At the device

HDX uses the computing capacity of user devices to enhance and optimize the user experience. HDX technology ensures that users receive a smooth, seamless experience with multimedia content in their virtual desktops or applications. Workspace control enables users to pause virtual desktops and applications and resume working from a different device at the point where they left off.

On the network

HDX incorporates advanced optimization and acceleration capabilities to deliver the best performance over any network, including low-bandwidth and high-latency WAN connections.

HDX features adapt to changes in the environment. The features balance performance and bandwidth. They apply the best technologies for each user scenario, whether the desktop or application is accessed locally on the corporate network or remotely from outside the corporate firewall.

In the data center

HDX uses the processing power and scalability of servers to deliver advanced graphical performance, regardless of the client device capabilities.

HDX channel monitoring provided by Citrix Director displays the status of connected HDX channels on user devices.

HDX Insight

HDX Insight is the integration of NetScaler Network Inspector and Performance Manager with Director. It captures data about ICA traffic and provides a dashboard view of real time and historical details. This data includes client-side and server-side ICA session latency, bandwidth use of ICA channels, and the ICA round-trip time value of each session.

You can enable NetScaler to use the HDX Insight virtual channel to move all the required data points in an uncompressed format. If you disable this feature, the NetScaler device decrypts and decompresses the ICA traffic spread across various virtual channels. Using the single virtual channel lessens complexity, enhances scalability, and is more cost effective.

Minimum requirements:

- Citrix Virtual Apps and Desktops 7 v1808
- XenApp and XenDesktop 7.17
- NetScaler version 12.0 Build 57.x
- Citrix Workspace app for Windows 1808
Citrix Virtual Apps and Desktops service

- Citrix Receiver for Windows 4.10
- Citrix Workspace app for Mac 1808
- Citrix Receiver for Mac 12.8

Enable or disable HDX Insight virtual channel

To disable this feature, set the Citrix NetScaler Application Flow service properties to Disabled. To enable, set the service to Automatic. In either case, we recommend that you restart the server machine after changing these properties. By default, this service is enabled (Automatic).

Experience HDX capabilities from your virtual desktop

- To see how browser content redirection, one of four HDX multimedia redirection technologies, accelerates delivery of HTML5 and WebRTC multimedia content:
  1. Download the Chrome browser extension and install it on the virtual desktop.
  2. To experience how browser content redirection accelerates the delivery of multimedia content to virtual desktops, view a video on your desktop from a website containing HTML5 videos, such as YouTube. Users don’t know when browser content redirection is running. To see whether browser content redirection is being used, drag the browser window quickly. You’ll see a delay or out of frame between the viewport and the user interface. You can also right-click on the webpage and look for About HDX Browser Redirection in the menu.
- To see how HDX delivers high definition audio:
  1. Configure your Citrix client for maximum audio quality; see the Citrix Workspace app documentation for details.
  2. Play music files by using a digital audio player (such as iTunes) on your desktop.

HDX provides a superior graphics and video experience for most users by default, and configuration
Citrix Virtual Apps and Desktops service

isn’t required. Citrix policy settings that provide the best experience for most use cases are enabled by default.

- HDX automatically selects the best delivery method based on the client, platform, application, and network bandwidth, and then self-tunes based on changing conditions.
- HDX optimizes the performance of 2D and 3D graphics and video.
- HDX enables user devices to stream multimedia files directly from the source provider on the internet or intranet, rather than through the host server. If the requirements for this client-side content fetching are not met, media delivery falls back to server-side content fetching and multimedia redirection. Usually, adjustments to the multimedia redirection feature policies aren’t needed.
- HDX delivers rich server-rendered video content to virtual desktops when multimedia redirection is not available: View a video on a website containing high definition videos, such as http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

Good to know:

- For support and requirements information for HDX features, see the System requirements article. Except where otherwise noted, HDX features are available for supported Windows Multi-session OS and Windows Single-session OS machines, plus Remote PC Access desktops.
- This content describes how to optimize the user experience, improve server scalability, or reduce bandwidth requirements. For information about using Citrix policies and policy settings, see the Citrix policies documentation for this release.
- For instructions that include editing the registry, use caution: 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.

Auto client reconnect and session reliability

When accessing hosted applications or desktops, network interruption might occur. To experience a smoother reconnection, we offer auto client reconnect and session reliability. In a default configuration, session reliability starts and then auto client reconnect follows.

Auto client reconnect:

Auto client reconnect relaunches the client engine to reconnect to a disconnected session. Auto client reconnect closes (or disconnects) the user session after the time specified in the setting. If auto client reconnect is in progress, the system sends application and desktops network interruption notification to the user as follows:

- **Desktops.** The session window is grayed out and a countdown timer shows the time until the reconnections occur.
• **Applications.** The session window closes and a dialog appears to the user containing a countdown timer showing the time until the reconnections are attempted.

During auto client reconnect, sessions relaunch expecting network connectivity. User cannot interact with sessions while auto client reconnect is in progress.

On reconnection, the disconnected sessions reconnect using saved connection information. The user can interact with the applications and desktops normally.

Default auto client reconnect settings:

- Auto client reconnect timeout: 120 seconds
- Auto client reconnect: Enabled
- Auto client reconnect authentication: Disabled
- Auto client reconnect Logging: Disabled

For more information, see Auto client reconnect policy settings.

**Session reliability:**

Session reliability reconnects ICA sessions seamlessly across network interruptions. Session reliability closes (or disconnects) the user session after the time specified in the setting. After the session reliability timeout, the auto client reconnect settings take effect, attempting to reconnect the user to the disconnected session. When session reliability is in progress, application and desktops network interruption notification are sent to the user as follows:

- **Desktops.** The session window becomes translucent and a countdown timer shows the time until the reconnections occur.
- **Applications.** The window becomes translucent along with connection interrupted pop ups from the notification area.

While session reliability is active, the user cannot interact with the ICA sessions. However, user actions like keystrokes are buffered for few seconds immediately after the network interruption and retransmitted when the network is available.

On reconnection, the client and the server resume at the same point where they were in their exchange of protocol. The session windows lose translucency and appropriate notification area pop ups are shown for applications.

Default session reliability settings

- Session reliability timeout: 180 seconds
- Reconnection UI opacity level: 80%
- Session reliability connection: Enabled
- Session reliability port number: 2598

For more information, see Session reliability policy settings.

**NetScaler with auto client reconnect and session reliability:**
If Multistream and Multiport policies are enabled on the server and any or all these conditions are true, auto client reconnect does not work:

- Session reliability is disabled on NetScaler Gateway.
- A failover occurs on the NetScaler appliance.
- NetScaler SD-WAN is used with NetScaler Gateway.

**HDX adaptive throughput**

HDX adaptive throughput intelligently fine-tunes the peak throughput of the ICA session by adjusting output buffers. The number of output buffers is initially set at a high value. This high value allows data to be transmitted to the client more quickly and efficiently, especially in high latency networks. Providing better interactivity, faster file transfers, smoother video playback, higher framerate and resolution results in an enhanced user experience.

Session interactivity is constantly measured to determine whether any data streams within the ICA session are adversely affecting interactivity. If that occurs, the throughput is decreased to reduce the impact of the large data stream on the session and allow interactivity to recover.

**Important:**
HDX adaptive throughput changes the way that output buffers are set by moving this mechanism from the client to the VDA, and no manual configuration is necessary.

This feature has the following requirements:

- VDA version 1811 or later
- Workspace app for Windows 1811 or later

**Improve the image quality sent to user devices**

The following visual display policy settings control the quality of images sent from virtual desktops to user devices.

- Visual quality. Controls the visual quality of images displayed on the user device: medium, high, always lossless, build to lossless (default = medium). The actual video quality using the default setting of medium depends on available bandwidth.
- Target frame rate. Specifies the maximum number of frames per second that are sent from the virtual desktop to the user device (default = 30). For devices that have slower CPUs, specifying a lower value can improve the user experience. The maximum supported frame rate per second is 60.
- Display memory limit. Specifies the maximum video buffer size for the session in kilobytes (default = 65536 KB). For connections requiring more color depth and higher resolution, increase the limit. You can calculate the maximum memory required.
Citrix Virtual Apps and Desktops service

**Improve video conference performance**

Several popular video conferencing applications are optimized for delivery from Citrix Virtual Apps and Desktops through multimedia redirection (see, for example, [HDX RealTime Optimization Pack](#)). For applications that are not optimized, HDX webcam video compression improves bandwidth efficiency and latency tolerance for webcams during video conferencing in a session. This technology streams webcam traffic over a dedicated multimedia virtual channel. This technology uses less bandwidth compared to the isochronous HDX Plug-n-Play USB redirection support, and works well over WAN connections.

Citrix Workspace app users can override the default behavior by choosing the Desktop Viewer Mic & Webcam setting **Don’t use my microphone or webcam**. To prevent users from switching from HDX webcam video compression, disable USB device redirection by using the policy settings under ICA policy settings > USB Devices policy settings.

HDX webcam video compression requires that the following policy settings be enabled (all are enabled by default).

- Client audio redirection
- Client microphone redirection
- Multimedia conferencing
- Windows Media Redirection

If a webcam supports hardware encoding, HDX video compression uses the hardware encoding by default. Hardware encoding might consume more bandwidth than software encoding. To force software compression, add the following DWORD key value to the registry key: HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

**Network traffic priorities**

Priorities are assigned to network traffic across multiple connections for a session using Quality of Service supported routers. Four TCP streams and two User Datagram Protocol (UDP) streams are available to carry ICA traffic between the user device and the server:

- TCP streams - real time, interactive, background, and bulk
- UDP streams - voice and Framehawk display remoting

Each virtual channel is associated with a specific priority and transported in the corresponding connection. You can set the channels independently, based on the TCP port number used for the connection.

Multiple channel streaming connections are supported for Virtual Delivery Agents (VDAs) installed on Windows 10, Windows 8, and Windows 7 machines. Work with your network administrator to ensure
the Common Gateway Protocol (CGP) ports configured in the Multi-Port Policy setting are assigned correctly on the network routers.

Quality of Service is supported only when multiple session reliability ports, or the CGP ports, are configured.

**Warning**

Use transport security when using this feature. Citrix recommends using Internet Protocol Security (IPsec) or Transport Layer Security (TLS). TLS connections are supported only when the connections traverse a NetScaler Gateway that supports multi-stream ICA. On an internal corporate network, multi-stream connections with TLS are not supported.

To set Quality of Service for multiple streaming connections, add the following Citrix policy settings to a policy (see [Multi-stream connections policy settings](#) for details):

- **Multi-Port policy** - This setting specifies ports for ICA traffic across multiple connections, and establishes network priorities.
  - Select a priority from the CGP default port priority list. By default, the primary port (2598) has a High priority.
  - Type more CGP ports in CGP port1, CGP port2, and CGP port3 as needed, and identify priorities for each. Each port must have a unique priority.

  Explicitly configure the firewalls on VDAs to allow the additional TCP traffic.

- **Multi-Stream computer setting** - This setting is disabled by default. If you use Citrix NetScaler SD-WAN with Multi-Stream support in your environment, you do not need to configure this setting. Configure this policy setting when using third-party routers or legacy Branch Repeaters to achieve the desired Quality of Service.

- **Multi-Stream user setting** - This setting is disabled by default.

For policies containing these settings to take effect, users must log off and then log on to the network.

**Show or hide the remote language bar**

The language bar displays the preferred input language in an application session. If this feature is enabled (default), you can show or hide the language bar from the **Advanced Preferences > Language bar** UI in Citrix Workspace app for Windows. By using a registry setting on the VDA side, you can disable client control of the language bar feature. If this feature is disabled, the client UI setting doesn’t take effect, and the per user current setting determines the language bar state. For more information, see [Improve the user experience](#).

To disable client control of the language bar feature from the VDA:
1. In the registry editor, navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`.
2. Create a DWORD value key, SeamlessFlags, and set it to 0x40000.

**Unicode keyboard mapping**

Non-Windows Citrix Receivers use the local keyboard layout (Unicode). If a user changes the local keyboard layout and the server keyboard layout (scan code), they might not be in sync and the output is incorrect. For example, User1 changes the local keyboard layout from English to German. User1 then changes the server-side keyboard to German. Even though both keyboard layouts are German, they might not be in sync causing incorrect character output.

**Enable or disable Unicode keyboard layout mapping**

By default, the feature is disabled on the VDA side. To enable the feature, toggle on the feature by using registry editor regedit on the VDA. Add the following registry key:

**KEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap**

Name: EnableKlMap
Type: DWORD
Value: 1

To disable this feature, set `EnableKlMap` to 0 or delete the `CtxKlMap` key.

**Enable Unicode keyboard layout mapping compatible mode**

By default, Unicode keyboard layout mapping automatically hooks some windows API to reload the new Unicode keyboard layout map when you change the keyboard layout on the server side. A few applications cannot be hooked. To keep compatibility, you can change the feature to compatible mode to support these non-hooked applications. Add the following registry key:

**HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap**

Name: DisableWindowHook
Type: DWORD
Value: 1

To use normal Unicode keyboard layout mapping, set `DisableWindowHook` to 0.
Adaptive transport

August 21, 2020

Introduction

Adaptive transport is a data transport mechanism for Citrix Virtual Apps and Desktops. It is faster, can scale, improves application interactivity, and is more interactive on challenging long-haul WAN and internet connections. Adaptive transport maintains high server scalability and efficient use of bandwidth. By using adaptive transport, ICA virtual channels automatically respond to changing network conditions. They intelligently switch the underlying protocol between the Citrix protocol called Enlightened Data Transport (EDT) and TCP to deliver the best performance. It improves data throughput for all ICA virtual channels including Thinwire display remoting, file transfer (Client Drive Mapping), printing, and multimedia redirection. The same setting is applicable for both LAN and WAN conditions.

When set to Preferred, data transport over EDT is used as primary and fallback to TCP. With the Citrix Workspace app for Windows minimum version 1808 or Citrix Receiver for Windows minimum version 4.10 and session reliability enabled, EDT and TCP are attempted in parallel during the initial connection, session reliability reconnection, and auto client reconnect. Doing so reduces connection time if EDT is Preferred, but the required underlying UDP transport is unavailable and TCP must be used. By default, after fallback to TCP, adaptive transport continues to seek EDT every five minutes.
**Important:**

EDT and TCP in parallel require:

- Citrix Workspace app for Windows minimum version 1808 and session reliability.
- Citrix Receiver for Windows minimum version 4.10 and session reliability.
- Citrix Workspace app for Mac minimum version 1808 and session reliability.
- Citrix Receiver for Mac minimum version 12.8 and session reliability.

By default, adaptive transport is enabled (**Preferred**), and EDT is used when possible, with fallback to TCP.

For testing purposes, you can set **Diagnostic mode**, in which case only EDT is used, and fallback to TCP is disabled.

---

**Interoperability with Citrix SD-WAN WAN optimization**

Citrix SD-WAN WAN optimization (WANOP) offers cross-session tokenized compression (data deduplication), including URL-based video caching. WANOP provides significant bandwidth reduction. This occurs if two or more people at the office location watch the same client-fetched video, or transfer or print significant portions of the same file or document. Furthermore, by running the processes for ICA data reduction and print job compression on the branch office appliance, WANOP offers VDA server CPU offload and enables higher Citrix Virtual Apps and Desktops server scalability.

**Important**

When using the WANOP feature of Citrix SD-WAN, there is no need to disable Adaptive Transport. WANOP will automatically put the HDX session into TCP data transport mode, since WANOP provides equivalent flow control to EDT and adds the benefits described in the previous paragraph. Non-WANOP sessions will use EDT whenever possible. By using TCP flow control and congestion control, WANOP ensures the equivalent interactivity to EDT at high latency and moderate packet
Requirements and considerations

- Citrix Virtual Apps and Desktops: Minimum version 7.1808.
- StoreFront: Minimum version 3.9.
- Citrix Workspace app for Windows minimum version 1808
- Citrix Receiver for Windows: Minimum version 4.7 (EDT and TCP in parallel require minimum version 4.10 and session reliability).
- Citrix Workspace app for Mac minimum version 1808
- Citrix Receiver for Mac: Minimum version 12.5 (EDT and TCP in parallel require minimum version 12.8 and session reliability).
- Citrix Workspace app for iOS minimum version 1808
- Citrix Receiver for iOS: Minimum version 7.2.
- Citrix Workspace app for Linux minimum version 1808
- Citrix Receiver for Linux: Minimum version 13.6 for Direct VDA Connections only and minimum version 13.7 for DTLS support using NetScaler Gateway (or DTLS for direct VDA connections).
- Citrix Workspace app for Android minimum version 1808
- Citrix Receiver for Android: Minimum version 3.12.3 for Direct VDA Connections only.
- IPv4 VDAs only. IPv6 and mixed IPv6 and IPv4 configurations are not supported.
- Citrix Gateway (Citrix ADC): Minimum versions 11.1 build 51.21, 12.0 build 35.6. We recommend minimum versions 11.1 build 55.10 or 12.0 Build 53.6 as these versions include important DTLS fragmentation fixes. For more information on configuration, see Configure Citrix Gateway to support Enlightened Data Transport and HDX Insight.

Configuration

1. Install Citrix Virtual Apps and Desktops.
2. Install StoreFront. If you are using Citrix Gateway, verify that session reliability is enabled. Do so in Studio > StoreFront > Manage NetScaler Gateway > Select your NetScaler > Secure Ticket Authority > Enable Session Reliability.
3. Install the VDA (for single-session OS or multi-session OS).
4. Install Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Workspace app for iOS, Citrix Workspace app for Android, or Citrix Workspace app for Linux.
5. If you are using Citrix Gateway, enable session reliability in the Studio policy. Also, enable DTLS in the front-end VPN virtual server.
6. In Studio, enable the policy setting, HDX Adaptive Transport (it is enabled by default).
   • To enable the policy setting, set the value to Preferred, then click **OK**.
     – **Preferred**. Adaptive transport over EDT is used when possible, with fallback to TCP.
     – **Diagnostic mode**. EDT is forced on and falls back to TCP is disabled. We recommend this setting only for troubleshooting.
     – **Off**. TCP is forced on, and EDT is disabled.
7. Click Next, and complete the steps in the wizard.
8. The policy takes effect when the user reconnects the ICA session. Though not required, you can run `gpupdate /force` to pull the policy setting to the server, but the user still has to reconnect the ICA session.
9. Start a session from a supported Citrix Workspace app to establish a connection using adaptive transport.
10. For secure external access, configure DTLS encryption on Citrix Gateway. For more information, see this article.

To confirm that the policy setting has taken effect:

   • Check that the ICA User Datagram Protocol (UDP) services are enabled on a VDA using `netstat -a`.
   • Check that the virtual channels are running over EDT using **Director** or the `CtxSession.exe` command-line utility available on the VDA.

**Director example:**

In Director, **Session Details > Connection Type** displays the policy settings. Look for Connection type **HDX**. If the protocol is **UDP**, EDT is active for the session. If the protocol is **TCP**, the session is in fallback or default mode. If the Connection type is **RDP**, ICA is not in use and the protocol is **n/a**. For more information, see Monitor sessions.
**CtxSession.exe example:**

This example illustrates that EDT over UDP is active for the session. Type CtxSession.exe in the command line.

C:\Program Files (x86)\Citrix\System32>CtxSession

Session 2 Transport Protocols: UDP -> CGP -> ICA

To see verbose statistics, use the -v switch:

>`CtxSession -v`
Troubleshoot EDT connections

Requirements and considerations

- Multi-session OS VDA 7.13
- Single-session OS VDA 7.13
- Receiver for Windows 4.7 (4.6 was Experimental)
- Receiver for Linux:
  - 13.6 (direct connections)
  - 13.7 (DTLS supported)
- Receiver for Mac 12.5
- Receiver for iOS 7.2
- Receiver for Android:
  - 3.12.3 (direct connections)
  - 3.13 (DTLS supported)
- StoreFront 3.9
- Citrix Gateway Release 11.1–51.21 / 12.0.53.6 or later

Parallel Connections

Receiver for Windows 4.10, Mac 12.8, and iOS 7.5 include code that allows them to attempt an EDT and TCP connection in parallel. EDT is given a 500 milliseconds head-start to favor UDP. Any VDA that supports EDT also supports the parallel connection.

To troubleshoot EDT connections, refer to the following procedure:

1. Verify the minimum product/component version requirements. See Requirements and considerations.

2. Check if the HDX adaptive transport policy in Studio is set to Not Configured or set to Preferred.

   Note:
   In XenApp and XenDesktop 7.16, HDX adaptive transport is Preferred by default and there is no explicit requirement to configure the Studio policy.

3. Check if the optional Receiver GPO Administrative Templates are used. If so, ensure that the Transport Protocol for Citrix Receiver value is set to Not Configured or Preferred. Receiver for Windows side configurations is optional.

4. Ensure that the UDP sockets are listening on the VDA. Open a command prompt in the VDA and type `netstat -a -p udp`. For details, see How to Confirm HDX Enlightened Data Transport Protocol.
5. Bypass the NetScaler Gateway: The best way to test EDT is to launch an app from the internal network directly to StoreFront, bypassing the NetScaler Gateway. Run `ctxsession` on the VDA command prompt and verify your session is using UDP. If that works, your VDA is also ready for EDT connections from the outside.

6. Launch a session through NetScaler Gateway, but first inspect the ICA file. Ensure there is an entry that reads `HDXoverUDP = Preferred`. If it is set to `Off`, then the HDX adaptive transport in not set to `Preferred` in the Studio policy, or the group policy update has not been applied yet at the VDA. There should also be an entry `CGPSecurityTicket=On`, where CGP is a requirement for EDT to work using the NetScaler Gateway.

7. In the NetScaler Gateway, run `ctxsession` on the VDA command prompt and verify that your session is using UDP. If it is set to TCP, something might be wrong between the Citrix Receiver and the NetScaler Gateway front-end virtual server, and the connection fell back to TCP.

8. Any NetScaler Gateway before 12.0.56.20 requires DTLS to be manually enabled on the front-end VPN virtual server.

9. If you are using a VPN like Cisco AnyConnect or any other solution that alters the MTU in the network, the EDT connections might fail. You must calculate the overhead introduced by the VPN vendor, and then modify the ICA file template in StoreFront to include two more entries. Also, add a Citrix Receiver-side change. For more details, see CTX231821.

**More troubleshooting tools**

- **Wireshark**: To troubleshoot if you can’t identify the problem, use a Wireshark trace on NetScaler Gateway to troubleshoot. Wireshark Dissectors can misinterpret EDT as QUIC. You can use the `Decode As` feature in Wireshark to decode QUIC as DTLS.

- **NMAP**: Use the `nmap -sU -p 443 <IP Address of your NSG>` to test if UDP packets are reaching the virtual server.

See a working versus non-working trace:
Citrix Virtual Apps and Desktops service

- **Director:** In addition, you can check **Citrix Director > Session Details > Protocol > UDP.**
- **CDF Traces:** You might need to check the EDT logic on XenApp and XenDesktop components, and generate CDF traces while reproducing the issue.

### Server CDF Traces

<table>
<thead>
<tr>
<th>Module</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICA Service</td>
<td>XenDesktop only</td>
</tr>
<tr>
<td>MF_DLL_WSXICA</td>
<td>RPM on XenApp only</td>
</tr>
<tr>
<td>MF_Driver_Wdica</td>
<td>Both</td>
</tr>
<tr>
<td>Portica_Driver_Picadd</td>
<td>Only needed for MSI</td>
</tr>
<tr>
<td>Portica_Driver_Td</td>
<td>This also includes traces from EDT, CGP, TLS/DTLS, HTML5, SOCKS (if HTML5 or TLS port, and CGP is not used)</td>
</tr>
<tr>
<td>CitrixServicesManager_Service</td>
<td>XenApp Only</td>
</tr>
<tr>
<td>StackControl_Agent_ToStack</td>
<td>XenApp Only</td>
</tr>
<tr>
<td>Broker Agent</td>
<td>Both</td>
</tr>
</tbody>
</table>

### Receiver CDF Traces

<table>
<thead>
<tr>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>icaClient_Engine_WficaCtlGuid</td>
</tr>
<tr>
<td>icaClient_UDT</td>
</tr>
</tbody>
</table>

### Loss tolerant mode

**Important:**
- The feature requires a minimum of Citrix Workspace app 2002 for Windows. This version of
Citrix Virtual Apps and Desktops service

the VDA will support it when it becomes available.

- Loss tolerant mode is not supported on Citrix Gateway or Citrix Gateway Service. This mode
  is available only with direct connections.

Loss tolerant mode enhances the user experience for users connecting through networks with high
latency and packet loss. It accomplishes this by using the EDT Lossy transport protocol.

Initially, sessions are established using EDT. If the latency and packet loss thresholds are reached or
surpassed, the applicable virtual channels switch from EDT to EDT Lossy, while leaving the other vir-
tual channels on EDT. If the latency and packet loss decrease below the thresholds, the applicable
virtual channels switch back to EDT.

The default thresholds are:

- Packet loss: 5%
- Latency: 300 ms (RTT)

Loss tolerant mode is enabled by default and can be disabled using the loss tolerant mode setting.
Adjust the packet loss and latency thresholds using the loss tolerant mode thresholds setting.

Requirements:

- Citrix Virtual Delivery Agent (VDA) 2003
- Citrix Workspace app 2002 for Windows
- Session reliability enabled. For more information about session reliability, see Session reliabil-
  ity policy settings.

EDT MTU Discovery

EDT automatically determines the Maximum Transmission Unit (MTU) when establishing a session.
Doing so prevents EDT packet fragmentation that might result in performance degradation or failure
to establish a session.

Minimum requirements:

- VDA minimum version 1912
- Citrix Workspace app 1911 for Windows
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- Session Reliability must be enabled

If using client platforms or versions that do not support this feature, see the Knowledge Center article
CTX231821 for details about how to configure a custom EDT MTU that is appropriate for your environ-
ment.
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.

To enable or disable EDT MTU Discovery on the VDA

1. Set this registry key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

   Name: MtuDiscovery
   Type: DWORD
   Data: 00000001

2. Restart the VDA and wait for the VDA to register.

To disable EDT MTU Discovery, delete this registry value and restart the VDA.

This setting is machine-wide and affects all sessions connecting from a supported client.

To control EDT MTU Discovery on the client

You can control EDT MTU Discovery selectively on the client by adding the MtuDiscovery parameter in the ICA file. To disable the feature, set the following under the Application section:

MtuDiscovery=Off

To re-enable the feature, remove the MtuDiscovery parameter from the ICA file.

Important:
For this ICA file parameter to work, enable the feature on the VDA. If the feature is not enabled on the VDA, the ICA file parameter has no effect.

Rendezvous protocol

June 1, 2020
In environments that use the Citrix Gateway service, the Rendezvous protocol allows HDX sessions to bypass the Citrix Cloud Connector and connect directly and securely to the Citrix Gateway service.

Requirements:

- **Access to environment using Citrix Workspace and Citrix Gateway service.**
- **Control Plane: Citrix Virtual Apps and Desktops Service (Citrix Cloud)**
- **VDA: Version 1912 or later.**
- **Enable the Rendezvous protocol in the Citrix policy.** For more information, see [Rendezvous protocol policy setting](#).
- **The VDAs must have access to** `https://*.nssvc.net`, including all subdomains. If you can’t whitelist all subdomains in that manner, use `https://*.c.nssvc.net` and `https://*.g.nssvc.net` instead. For more information, see the [Internet Connectivity Requirements](#) section of the Citrix Cloud documentation (under Virtual Apps and Desktop service) and the Knowledge Center article [CTX270584](#).
- **Cloud Connectors must obtain the VDAs’ FQDNs when brokering a session.** Accomplish this in one of these two ways:
  - **Enable DNS resolution for the site.** Using the Citrix Virtual Apps and Desktops Remote PowerShell SDK, run the command `Set-BrokerSite -DnsResolutionEnabled $true`. For more information about the Citrix Virtual Apps and Desktops Remote PowerShell SDK, see [SDKs and APIs](#).
  - **DNS Reverse Lookup Zone with PTR records for the VDAs.** If you choose this option, we recommend that you configure VDAs to always attempt to register PTR records. To do so, use the Group Policy Editor or Group Policy Object, navigate to **Computer Configuration > Administrative Templates > Network > DNS Client**, and set **Register PTR Records** to **Enabled and Register**.

- **On the VDA, configure the SSL Cipher Suite Order.** Use the Group Policy Editor or Group Policy Object. Under the **Computer Configuration** node, go to **Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order**.

  **Important:**

  **Rules for SSL Cipher Suite:**

  The SSL Cipher Suite order list must be in strict comma delimited format.

  Except for the last string, each string must end with a comma (,).

  Do not add spaces.

  If the VDA machines are non-persistent (that is, provisioned with MCS or PVS), configure the cipher suite order in the master image.
Select this order:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

Important:
The Rendezvous protocol doesn't support transparent or explicit proxies. To use proxies, continue to use the Cloud Connector for ICA traffic.

If you enable Rendezvous and the VDA can’t reach the Citrix Gateway service directly, the VDA falls back to proxy the HDX session through the Cloud Connector.

If you meet all requirements, follow these steps to validate if Rendezvous is in use:

1. Launch PowerShell or a command prompt within the HDX session.
2. Run `ctxsession.exe -v`.
3. Note the local address. If Rendezvous is in use, the local address is `0.0.0.0` followed by a 5-digit port number (for example, `0.0.0.0:50343`).

This diagram is an overview of the Rendezvous connection flow. Follow the steps to understand the flow.

1. Navigate to Citrix Workspace
2. Enter credentials in Citrix Workspace.
3. If using on-premises Active Directory, the Citrix Virtual Apps and Desktops service authenticates credentials with Active Directory using the Cloud Connector channel.
4. Citrix Workspace displays enumerated resources from the Citrix Virtual Apps and Desktop service.
5. Select resources from Citrix Workspace. The Citrix Virtual Apps and Desktop service sends a message to the VDA to prepare for an incoming session.
6. Citrix Workspace sends an ICA file to the endpoint that contains an STA ticket generated by Citrix Cloud.
7. The endpoint connects to the Citrix Gateway service, provides the ticket to connect to the VDA, and Citrix Cloud validates the ticket.
8. The Citrix Gateway service sends connection information to the Cloud Connector. The Cloud Connector determines if the connection is supposed to be a Rendezvous connection and sends the information to the VDA.
9. The VDA establishes a direct connection to the Citrix Gateway service.
10. If a direct connection between the VDA and the Citrix Gateway service isn’t possible, the VDA proxies its connection the Cloud Connector.
11. The Citrix Gateway service establishes a connection between the endpoint device and the VDA.
12. The VDA verifies its license with the Citrix Virtual Apps and Desktop service through the Cloud Connector.
13. The Citrix Virtual Apps and Desktop service sends session policies to the VDA through the Cloud Connector. Those policies are applied.

Copied!
Failed!

**Citrix ICA virtual channels**

August 21, 2020

**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.

**What are ICA virtual channels?**

A large portion of the functionality and communication between the Citrix Workspace app and the Citrix Virtual Apps and Desktops servers occurs over virtual channels. Virtual channels are a necessary part of the remote computing experience with the Citrix Virtual Apps and Desktops servers. Virtual channels are used for:

- Audio
Citrix Virtual Apps and Desktops service

- COM ports
- Disks
- Graphics
- LPT ports
- Printers
- Smart cards
- Third-party custom virtual channels
- Video

New virtual channels are sometimes released with new versions of the Citrix Virtual Apps and Desktops servers and Citrix Workspace app products to provide more functionality.

A virtual channel consists of a client-side virtual driver that communicates with a server-side application. Citrix Virtual Apps and Desktops ship with various virtual channels included. They’re designed to allow customers and third-party vendors to create their own virtual channels by using one of the provided Software Development Kits (SDKs).

Virtual channels provide a secure way to accomplish various tasks. For example, an application that is running on a Citrix Virtual Apps server that is communicating with a client-side device or an application that is communicating with the client-side environment.
On the client side, virtual channels correspond to virtual drivers. Each virtual driver provides a specific function. Some are required for normal operation, and others are optional. Virtual drivers operate at the presentation layer protocol level. There can be several protocols active at any time by multiplexing channels that are provided by the Windows Station (WinStation) protocol layer.

The following functions are contained in the VirtualDriver registry value under this registry path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0
```

or

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0 (for 64-bit)
```

- Thinwire3.0 (Required)
- ClientDrive
- ClientPrinterQueue
- ClientPrinterPort
- Clipboard
- ClientComm
- ClientAudio
- LicenseHandler (Required)
- TWI (Required)
- SmartCard
- ICACTL (Required)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

**Note:**

You can disable specific client functionality by removing one or more of these values from the registry key. For example, if you wanted to remove the Client Clipboard, remove the word `Clipboard`.

This list contains the client virtual driver files and their respective functions. Citrix Virtual Apps and Citrix Workspace app for Windows use these files. They are in the form of Dynamic Link Libraries (user mode), and not Windows drivers (kernel mode) except for Generic USB as described in Generic USB virtual channel.

- `vd3dn.dll` – Direct3D virtual channel used for desktop composition redirection
- `vdcamN.dll` – Bidirectional audio
- `vdcdm30n.dll` – Client drive mapping
- `vdcmd30n.dll` - Client COM port mapping
• vdcpm30N.dll – Client printer mapping
• vdctlN.dll – ICA controls channel
• vddvcoN.dll – Dynamic virtual channel
• vdeuemn.dll - End user experience monitoring
• vdgusbn.dll – Generic USB virtual channel
• vdkbhook.dll – Transparent key pass-through
• vdlfpn.dll – Framehawk display channel over UDP like transport
• vdmmn.dll – Multimedia support
• vdmrvc.dll – Mobile Receiver virtual channel
• vdmtnn.dll - Multi-touch support
• vdsardn.dll – Smartcard support
• vdsens.dll – Sensors virtual channel
• vdspl30n.dll – Client UPD
• vdsspin.dll – Kerberos
• vdmtnn.dll – Transparent UI
• vdtw30n.dll – Client Thinwire
• vdmtnn.dll – Seamless
• vdmtnn.dll – Twain

Some virtual channels are compiled into other files. For example Clipboard Mapping is available in wfica32.exe

**64-bit compatibility**

Citrix Workspace app for Windows is 64-bit compatible. As with most of the binaries compiled for 32 bit, these client files have 64-bit compiled equivalents:

• brapi64.dll
• confmgr.dll
• ctxlogging.dll
• ctxmui.dll
• icacnf.exe
• icacnfs.dll
• icafie.dll
• pnipcn64.dll
• pnsson.dll
• ssoncom.exe
• ssonstub.dll
• vdkbhook64.dll
Generic USB virtual channel

Generic USB virtual channel implementation uses two kernel mode drivers along with virtual channel driver vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

How ICA virtual channels work

Virtual channels are loaded in multiple ways. The Shell (WfShell for the server and PicaShell for the workstation) load some virtual channels. Some virtual channels are hosted as windows services.

Virtual channel modules loaded by the Shell, for example:

- EUEM
- Twain
- Clipboard
- Multimedia
- Seamless session sharing
- Time Zone

Some are loaded as kernel mode, for example:

- CtxDvcs.sys – Dynamic virtual channel
- Icausbb.sys – Generic USB redirection
- Picadm.sys – Client drive mapping
- Picaser.sys – COM port redirection
- Picapar.sys – LPT port redirection

Graphics virtual channel on the server side

Starting with XenApp 7.0 and XenDesktop 7.0, ctxgfx.exe hosts the graphics virtual channel for both workstation and terminal server based sessions. Ctxgfx hosts platform specific modules that interact with the corresponding driver (Icardd.dll for RDSH and vdod.dll and vidd.dll for workstation).

For XenDesktop 3D Pro deployments an OEM graphics driver is installed for the corresponding GPU on the VDA. Ctxgfx loads specialized adaptor modules to interact with the OEM graphics driver.

Hosting specialized channels in windows services

On Citrix Virtual Apps and Desktops servers, various channels are hosted as windows services. Such hosting provides one-to-many semantics for multiple applications in a session and multiple sessions on the server. Examples of such services include:
Citrix Virtual Apps and Desktops service

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service (Citrix Virtual Desktops only)

The audio virtual channel on Citrix Virtual Apps is hosted using Windows Audio service.

On the server side, all client virtual channels are routed through the WinStation driver, Wdica.sys. On the client side, the corresponding WinStation driver, built into wfica32.exe, polls the client virtual channels. This image illustrates the virtual channel client-server connection.

This overview contains a client-server data exchange using a virtual channel.

1. The client connects to the Citrix Virtual Apps and Desktops server. The client passes information about the virtual channels it supports to the server.

2. The server-side application starts, obtains a handle to the virtual channel, and optionally queries for additional information about the channel.
3. The client virtual driver and server-side application pass data using the following two methods:

   • If the server application has data to send to the client, the data is sent to the client immediately. When the client receives the data, the WinStation driver de-multiplexes the virtual channel data from the ICA stream and immediately passes it to the client virtual driver.

   • If the client virtual driver has data to send to the server, the data is sent the next time the WinStation driver polls it. When the server receives the data, it is queued until the virtual channel application reads it. There is no way to alert the server virtual channel application that data was received.

4. When the server virtual channel application is completed, it closes the virtual channel and frees any allocated resources.

**Creating your own virtual channel using the Virtual Channel SDK**

Creating a virtual channel using the Virtual Channel SDK requires intermediate programming knowledge. Use this method to provide a major communication path between the client and the server. For example, if you are implementing usage of a device on the client side, such as a scanner, to be used with a process in the session.

**Notes:**

   • The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.

   • Because of enhanced security for Citrix Virtual Apps and Desktops and Citrix Workspace app for Windows, you must take an extra step when installing a custom virtual channel.

**Creating your own virtual channel using the ICA Client Object SDK**

Creating a virtual channel using the ICA Client Object (ICO) is easier than using the Virtual Channel SDK. Use the ICO by creating a named object in your program using the `CreateChannels` method.

**Important:**

Because of enhanced security starting with the 10.00 version of the Citrix Receiver for Windows and later (and Citrix Workspace apps for Windows), you must take an extra step when creating an ICO virtual channel.

For more information, see [Client Object API Specification Programmer’s Guide](#).
Pass-through functionality of virtual channels

Most virtual channels that Citrix provides operate unmodified when you use the Citrix Workspace app for Windows within an ICA session (also known as a pass-through session). There are considerations when using the client in extra hops.

The following functions operate the same way in single or multiple hops:

- Client COM port mapping
- Client drive mapping
- Client printer mapping
- Client UPD
- End user experience monitoring
- Generic USB
- Kerberos
- Multimedia support
- Smartcard support
- Transparent key pass-through
- Twain

As the inherent nature of latency and factors such as compression and decompression and rendering being performed at each hop, performance might be affected with each additional hop that the client undergoes. The affected areas are:

- Bidirectional audio
- File transfers
- Generic USB redirection
- Seamless
- Thinwire

Important:

By default, the client drives mapped by an instance of the client running in a pass-through session are restricted to the client drives of the connecting client.

Pass-through functionality of virtual channels between a Citrix Virtual Desktop session and a Citrix Virtual App session

Most virtual channels provided by Citrix operate unmodified when you use Citrix Workspace app for Windows within an ICA session on a Citrix Virtual Desktops server (also known as a pass-through session).

Specifically, on the Citrix Virtual Desktops server, there is a VDA hook that runs picaPassthruHook. This hook makes the client think it’s running on a CPS server, and placing the client into its traditional
pass-through mode.

We support the following traditional virtual channels and their functionality:

- Client
- Client COM port mapping
- Client drive mapping
- Client printer mapping
- Generic USB (limited due to performance)
- Multimedia support
- Smartcard support
- SSON
- Transparent key pass-through

Security and ICA virtual channels

Securing usage is an important part of planning, developing, and implementing virtual channels. There are several references to specific areas of security located throughout this document.

Best practices

Open virtual channels when you Connect and Reconnect. Close virtual channels when you log off and Disconnect.

Keep the following guidelines in mind when you create scripts that use virtual channel functions.

Naming the Virtual Channels:

You can create a maximum of 32 virtual channels. Seventeen of the 32 channels are reserved for special purposes.

- Virtual channel names must not be more than seven characters in length.
- The first three characters are reserved for the vendor name, and the next four for the channel type. For example, CTXAUD represents the Citrix audio virtual channel.

Virtual channels are referred to by a seven-character (or shorter) ASCII name. In some previous versions of the ICA protocol, virtual channels were numbered. The numbers are now assigned dynamically based on the ASCII name, making implementation easier. Users who are developing virtual channel code for internal use only can use any seven-character name that does not conflict with existing virtual channels. Use only numbers and upper and lowercase ASCII. Follow the existing naming convention when adding your own virtual channels. There are several predefined channels. The predefined channels begin with the OEM identifier CTX and are for use only by Citrix.

Double-Hop Support:
## Virtual Channel

<table>
<thead>
<tr>
<th>Virtual Channel</th>
<th>Is double hop supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>No</td>
</tr>
<tr>
<td>Browser ContentRedirection</td>
<td>No</td>
</tr>
<tr>
<td>CDM</td>
<td>Yes</td>
</tr>
<tr>
<td>CEIP</td>
<td>No</td>
</tr>
<tr>
<td>Clipboard</td>
<td>Yes</td>
</tr>
<tr>
<td>Continuum (MRVC)</td>
<td>No</td>
</tr>
<tr>
<td>Control VC</td>
<td>Yes</td>
</tr>
<tr>
<td>HTML5 Video Redirection (v1)</td>
<td>Yes</td>
</tr>
<tr>
<td>Keyboard, Mouse</td>
<td>Yes</td>
</tr>
<tr>
<td>MultiTouch</td>
<td>No</td>
</tr>
<tr>
<td>NSAPVC</td>
<td>No</td>
</tr>
<tr>
<td>Printing</td>
<td>Yes</td>
</tr>
<tr>
<td>SensVC</td>
<td>No</td>
</tr>
<tr>
<td>Smartcard</td>
<td>Yes</td>
</tr>
<tr>
<td>Twain</td>
<td>Yes</td>
</tr>
<tr>
<td>USB VC</td>
<td>Yes</td>
</tr>
<tr>
<td>WAYCOM devices -K2M using USB VC</td>
<td>Yes</td>
</tr>
<tr>
<td>Webcam Video Compression</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Media Redirection</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### See also

- **ICA Virtual Channel SDK**
- **The Citrix Developer Network** is the home for all technical resources and discussions involving the use of Citrix SDKs. In this network, you can find access to SDKs, sample code and scripts, extensions and plug-ins, and SDK documentation. Also included are the Citrix Developer Network forums, where technical discussions take place around each of the Citrix SDKs.
Double hop in Citrix Virtual Apps and Desktops

August 14, 2020

In the context of a Citrix client session, the term “double hop” refers to a Citrix Virtual App session that is running within a Citrix Virtual Desktop session. The following diagram illustrates a double hop.

In a double hop scenario, when the user connects to a Citrix Virtual Desktop running on a single-session OS VDA (known as VDI) or a multi-session OS VDA (known as a published desktop), that is considered the first hop. After the user connects to the virtual desktop, the user can launch a Citrix Virtual Apps session. That is considered the second hop.

You can use a double hop deployment model to support various use cases. The case where the Citrix Virtual Desktop and the Citrix Virtual Apps environments are managed by different entities is one common example. This method can also be effective in resolving application compatibility issues.

System requirements

All Citrix Virtual Apps and Desktop editions including the Citrix Cloud service support double hop.

The first hop must use a supported version of the single-session or multi-session OS VDA and the Citrix Workspace App. The second hop must use a supported version of the multi-session OS VDA. See the Product Matrix page for supported versions.

For best performance and compatibility, Citrix recommends using a Citrix client of the same version or newer than the VDA versions in use.

In environments where the first hop involves a third-party (non-Citrix) virtual desktop solution in combination with a Citrix Virtual Apps session, support is limited to the Citrix Virtual Apps environment. In the event of any issues related to the third-party virtual desktop, including - but not limited to - Citrix Workspace app compatibility, redirection of hardware devices, and session performance, Citrix can provide technical support in a limited capacity. A Citrix Virtual Desktop at the first hop might be required as part of troubleshooting.

Deployment considerations for HDX in double hop

In general, each session in a double hop is unique and client-server functions are isolated to a given hop. This section includes areas that require special consideration by Citrix administrators. Citrix recommends that customers conduct thorough testing of required HDX capabilities to ensure user experience and performance is adequate for a given environment configuration.
Citrix Virtual Apps and Desktops service

**Graphics**

Use default graphics settings (selective encoding) on the first and second hops. In the case of **HDX 3D Pro**, Citrix highly recommends that all applications that require graphics acceleration run locally in the first hop with the appropriate GPU resources available to the VDA.

**Latency**

End-to-end latency can impact the overall user experience. Consider the added latency between the first and second hops. This is especially important with redirection of hardware devices.

**Multimedia**

Server-side (in session) rendering of audio and video content performs best in the first hop. Video playback in the second hop requires decoding and re-encoding at the first hop, increasing bandwidth and hardware resource utilization as a result. Audio and video content must be limited to the first hop whenever possible.

**USB device redirection**

HDX includes generic and optimized redirection modes to support a wide array of USB device types. Pay special attention to the mode in use at each hop and use the following table as reference for best results. For more information about generic and optimized redirection modes, see **Generic USB devices**.

<table>
<thead>
<tr>
<th>First hop (VDI or published desktop)</th>
<th>Second hop (Virtual apps)</th>
<th>Support notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimized</td>
<td>Optimized</td>
<td>Recommended (based on device support). For example, USB mass storage, TWAIN scanners, Webcam, Audio.</td>
</tr>
<tr>
<td>Generic</td>
<td>Generic</td>
<td>For devices where the optimized option is not available.</td>
</tr>
<tr>
<td>Generic</td>
<td>Optimized</td>
<td>While technically possible, it is recommended to use the optimized mode across both hops when device support is available.</td>
</tr>
</tbody>
</table>
First hop (VDI or published desktop) | Second hop (Virtual apps) | Support notes
---|---|---
Optimized | Generic | Not supported

Note:
Due to the inherent chattiness of USB protocols, performance may decrease across hops. Functionality and results vary depending on specific device and application requirements. Validation testing is highly recommended in all cases of device redirection and especially important in double hop scenarios.

Support exceptions

Double hop sessions support most HDX features and capabilities except for the following:

- Browser content redirection
- Local App Access
- RealTime Optimization Pack for Skype for Business
- Optimization for Microsoft Teams

Devices

April 7, 2020

HDX provides a high-definition user experience on any device, at any location. The articles in the Devices section describe these devices:

- Generic USB device
- Mobile and touch screen devices
- Serial devices
- Specialty keyboards
- TWAIN devices
- Webcams
Optimized vs. generic USB device

An optimized USB device is one for which Citrix Workspace app has specific support. For example, the ability to redirect webcams using the HDX Multimedia virtual channel. A generic device is a USB device for which there is no specific support in Citrix Workspace app.

By default, generic USB redirection can’t redirect USB devices with optimized virtual channel support unless put into Generic mode.

In general, you get better performance for USB devices in Optimized mode than in Generic mode. However, there are cases where a USB device doesn’t have full functionality in Optimized mode. It might be necessary to switch to Generic mode to gain full access to its features.

With USB mass storage devices, you can use either client drive mapping or generic USB redirection, or both, controlled by Citrix polices. The main differences are:

If both generic USB redirection and the client drive mapping policies are enabled and a mass storage device is inserted either before or after a session starts, it’s redirected using client drive mapping.

When these conditions are true, the mass storage device is redirected using generic USB redirection:

- Both generic USB redirection and the client drive mapping policies are enabled.
- A device is configured for automatic redirection.
- A mass storage device is inserted either before or after a session starts.

For more information, see [http://support.citrix.com/article/CTX123015](http://support.citrix.com/article/CTX123015).

<table>
<thead>
<tr>
<th>Feature</th>
<th>Client drive mapping</th>
<th>Generic USB redirection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled by default</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Read-only access</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>configurable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted device access</td>
<td>Yes, if encryption is unlocked before the device is accessed on the virtual session.</td>
<td>Citrix Virtual Desktops only</td>
</tr>
</tbody>
</table>

Mixed DPIs with multi-monitors

Citrix Virtual Apps and Desktops environments do not support the use of different DPIs between monitors. You can verify the DPI (% scaling) using Windows Control Panel > Display options. If using a Windows 8.1 or Windows 10 client device, enabling the Let me choose one scaling level for all my displays option in the Windows Control Panel > Display options configures the monitors appropriately. For more information, see Knowledge Center article [CTX201696](http://support.citrix.com/article/CTX201696).
Generic USB devices

April 7, 2020

HDX technology provides **optimized support** for most popular USB devices. These devices include:

- Monitors
- Mice
- Keyboards
- Voice over Internet Protocol phones
- Headsets
- Webcams
- Scanners
- Cameras
- Printers
- Drives
- Smart card readers
- Drawing tablets
- Signature pads

Optimized support offers an improved user experience with better performance and bandwidth efficiency over a WAN. Optimized support is usually the best option, especially in high latency or security-sensitive environments.

HDX technology provides **generic USB redirection** for specialty devices that don’t have optimized support or where it is unsuitable. For more information about generic USB redirection, see [Generic USB redirection](#).

For more information about USB devices and Citrix Workspace app for Windows, see [Configuring composite USB device redirection](#) and [Configuring USB support](#).

Mobile and touch screen devices

August 19, 2020
Tablet mode for touch screen devices using Windows Continuum

Continuum is a Windows 10 feature that adapts to the way the client device is used. This version of Continuum support, including dynamic change of modes, is available starting at VDA version 7.16 and Citrix Receiver for Windows version 4.10.

Windows 10 VDA detects the presence of a keyboard or mouse on a touch enabled client and puts the client in to desktop mode. If a keyboard or mouse is not present, Windows 10 VDA puts the client in to tablet/mobile mode. This detection occurs on connection and reconnection. It also occurs at dynamic attachment or detachment of the keyboard or mouse.

The feature is enabled by default. To disable this version of the feature, edit the Tablet mode toggle policy settings in the ICA policy settings article.

For the feature version included in XenApp 7.14 and 7.15 LTSR and XenDesktop 7.14 and 7.15 LTSR, use the registry settings to disable the feature. For more information, see Tablet mode for touch screen devices.

The tablet mode offers a user interface that is better suited to touch screens:

- Slightly larger buttons.
- The Start screen and any apps you start open in a full screen.
- Taskbar contains a back button.
- Icons deleted from the task bar.

You have access to the File Explorer.

The desktop mode offers the traditional user interface where you interact in the same manner as using PC and a keyboard and mouse.

Tablet mode requires a minimum of version XenServer 7.2. XenServer 7.2 integrates with the Citrix Virtual Desktops VDA, changing the hypervisor to enable the virtual firmware settings for 2-in-1 devices. Windows 10 loads the GPIO driver on the target virtual machine based on this updated BIOS. It is used for toggling between tablet and desktop modes within the virtual machine. For more information, see the release notes.

Citrix Workspace app for HTML5 (the light version) does not support Windows Continuum features.
Run the XenServer CLI command to allow laptop/tablet switching:

```
xevm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1
```

Important:
Updating the base image for an existing machine catalog after changing the metadata setting doesn't affect any previously provisioned VMs. After changing the XenServer VM base image, create a catalog, choose the base image, and provision a new Machine Creation Services (MCS) machine.

**Before starting a session:**

We recommend that you navigate to **Settings > System > Tablet Mode** on the VDA before starting a session and set the following options from the drop-down menus:

- Use the appropriate mode for my hardware
- Don't ask me and always switch

If you don’t set these options before starting the session, set the options after you start the session and restart the VDA.
Tablet mode

When I sign in

Use the appropriate mode for my hardware

When this device automatically switches tablet mode on or off

Don’t ask me and always switch

Microsoft Surface Pro and Surface Book pens

We support standard pen functionality with Windows Ink-based applications. This functionality requires a Virtual Delivery Agent running on a minimum of Microsoft Windows 10 version 1809 and client devices using a minimum of Citrix Workspace app for Windows version 1902. Support includes pointing, erasing, pen pressure, Bluetooth signals, and other features depending on the operating system firmware and pen model. For example, pen pressure can be up to 4096 levels. This feature is enabled by default.

For a demonstration of Windows Ink and the pen functionality, click this graphic:

![Showcasing Windows Ink in a Virtual Environment](image)

System requirements

- Citrix Virtual Apps and Desktops minimum version 1903
Citrix Virtual Apps and Desktops service

- Citrix Workspace app for Windows minimum version 1902
- Microsoft Windows 10 minimum version 1809

**Disable or enable**

To disable or enable this feature, set the following registry:

HKEY_LOCAL_MACHINE\Software\Citrix\Citrix Virtual Desktop Agent\PenApi

Name: DisablePen
Type: DWORD
Value:

1 - disables
0 - enables

*Copied!
*Failed!

**Serial ports**

August 21, 2020

Most new PCs don’t have built-in serial (COM) ports. The ports are easy to add by using USB converters. Applications suited for serial ports often involve sensors, controllers, old check readers, pads, and so forth. Some USB virtual COM-port devices use vendor-specific drivers in place of the Windows-provided drivers (usbser.sys). These drivers allow you to force the virtual COM port of the USB device so that it doesn’t change even if connected to different USB sockets. This might be done from the Device Manager > Ports (COM & LPT) > Properties or from the application that controls the device.

Client COM port mapping allows devices attached to the COM ports on the user’s endpoint to be used during virtual sessions. You can use these mappings like any other network mappings.

For each COM port, a driver in the operating system assigns a symbolic link name such as COM1 and COM2. The applications then use the link to access the port.

**Important:**

Because a device can attach to the endpoint by using USB directly, doesn’t mean it can be redirected using generic USB redirection. Some USB devices function as virtual COM ports, which applications can access in the same way as physical serial port. The operating system can abstract COM ports and treat them like fileshares. Two common protocols for virtual COM are CDC
When connected through an RS-485 port, applications might not work at all. Get an RS-485-to-RS232 converter to use RS-485 as a COM port.

Important:
Some applications recognize the device (for example, a signature pad) consistently only if it is connected to COM1 or COM2 on the client workstation.

Map a client COM port to a server COM port

You can map client COM ports to a Citrix session in three ways:

- Studio policies. For more information about policies, see Port redirection policy settings.
- VDA command prompt.
- Remote Desktop (Terminal Services) configuration tool.

1. Enable the Client COM port redirection and the Auto connect client COM ports Studio policies. After applied, some information is available in HDX Monitor.

2. If Auto connect client COM ports failed to map the port, you can map the port manually or use logon scripts. Log on to the VDA, and at a command prompt window, type:

   NET USE COMX: \CLIENT\COMZ:

   Or

   NET USE COMX: \CLIENT\CLIENTPORT:COMZ:

   X is the number of the COM port on the VDA (ports 1 through 9 are available for mapping). Z is the number of the client COM port you want to map.

   To confirm that the operation was successful, type NET USE at a VDA command prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports.
3. To use this COM port in a virtual desktop or application, install your user device application and point it to the mapped COM port name. For example, if you map COM1 on the client to COM3 on the server, install your COM port device application in the VDA and point it to COM3 during the session. Use this mapped COM port as you would a COM port on the user device.

**Important:**
COM port mapping is not TAPI-compatible. You can’t map Windows Telephony Application Programming Interface (TAPI) devices to client COM ports. TAPI defines a standard way for applications to control telephone functions for data, fax, and voice calls. TAPI manages signaling, including dialing, answering, and ending calls. Also, supplemental services such as holding, transferring, and conference calls.

**Troubleshoot**

1. Ensure you can access the device directly from the endpoint, bypassing Citrix. While the port is not mapped to the VDA, you are not connected to a Citrix session. Follow any troubleshooting instructions that came with the device and verify that it works locally first.

When a device is connected to a serial COM port, a registry key is created on the hive shown here:

You can also find this information from the command prompt by running `chgport /query`.
If troubleshooting instructions for the device aren’t available, try opening a PuTTY session. Choose **Session** and in **Serial line** specify your COM Port.
You can run **MODE** in a local command window. The output might display the COM port in use and the Baud/Parity/Data Bits/Stop Bits, which you need in your PuTTY session. If the PuTTY connection is successful, press **Enter** to see feedback from the device. Whatever characters you type might be repeated on the screen, or responded to. If this step is unsuccessful, you can’t access the device from a virtual session.

2. Map the local COM port to the VDA (using policies or **NET USE COMX: \CLIENT\COMZ:**) and repeat the same PuTTY procedures in the previous step, but this time from the VDA PuTTY. If PuTTY fails to show the error **Unable to open connection to COM1. Unable to open serial port**, another device might be using COM1.

3. Run **chgport /query**. If the built-in Windows serial driver on the VDA is auto-assigning \Device\Serial0 to a COM1 port of your VDA, do the following:
   A. Open CMD on the VDA and type **NET USE**.
   B. Delete any existing mapping (for example, COM1) on the VDA.

   **NET USE COM1 /DELETE**

   C. Map the device to the VDA.

   **NET USE COM1: \CLIENT\COM3:**

   D. Point your application on the VDA to COM3.

   Lastly, try to map your local COM port (for example, COM3) to a different COM port on the VDA (other than COM1, for example COM3). Ensure that your application is pointing to it:

   **NET USE COM3: \CLIENT\COM3**

4. If now you do see the port mapped, PuTTY is working but no data passing, it might be a race condition. The application might connect and open the port before it is mapped, locking it from being mapped. Try one of the following:
   - Open a second application published on the same server. Wait a few seconds for the port to be mapped, and then open the real application that tries to use the port.
• Enable the COM port redirection policies from the Group Policy Editor in Active Directory instead of Studio. Those policies are **Client COM port redirection** and **Auto connect client COM ports**. Policies applied this way might be processed before the Studio policies, guaranteeing that the COM port is mapped. Citrix policies are pushed to the VDA and stored in: \HKLM\SOFTWARE\Policies\Citrix \<user session ID>\>

• Use this logon script for the user or instead of publishing the application, publish a .bat script that first deletes any mapping on the VDA, remaps the virtual COM port, and then starts the application:

```bash
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \CLIENT\COM1:
NET USE COM2: \CLIENT\COM2:
MODE COM1: BAUD=1200 (or whatever value needed)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (or whatever value needed)
START C:\Program Files\<Your Software Path>\your_software.exe
```

5. Process Monitor from Sysinternals is the tool of last resort. When running the tool on the VDA, find and filter objects like COM3, picaser.sys, CdmRedirector, but especially `<your_app>.exe`. Any errors might appear as Access Denied or similar.

**Specialty keyboards**

August 21, 2020

**Bloomberg keyboards**

**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.

Citrix Virtual Apps and Desktops support the Bloomberg model 4 Starboard keyboard (and earlier model 3). This keyboard enables customers in the financial sector to use the special features of the keyboard to access financial market data and perform trading quickly.
This keyboard is compatible with the KVM switch boxes and can work in two modes:

- PC (One USB cable with no KVM)
- KVM mode (Two USB Cables with one routed through KVM)

**Important:**
We recommend that you use the Bloomberg keyboard with only one session. We don’t recommend using the keyboard with multiple concurrent sessions (one client to multiple sessions).

The Bloomberg keyboard 4 is a USB composite device comprising four USB devices in one physical shell:

- Keyboard.
- Fingerprint reader.
- Audio device with keys to increase and decrease volume and mute the speaker and the microphone. This device includes onboard speaker, microphone, and jack for the microphone and headset.
- USB hub to connect all of these devices to the system.

**Requirements:**

- The session to which Citrix Workspace app for Windows is connecting must support USB devices.
- Minimum of Citrix Workspace app 1808 for Windows or Citrix Receiver for Windows 4.8 to support Bloomberg keyboard model 3 and 4.
- Minimum of Citrix Workspace app 1808 for Windows or Citrix Receiver for Windows 4.12 to use KVM mode (two USB cables with one routed through KVM) for Model 4.

For information about configuring Bloomberg keyboards on Citrix Workspace app for Windows, see Configuring Bloomberg keyboards.

**Enable Bloomberg keyboard support:**

By default, the support for the enhanced Bloomberg keyboard is disabled. Enable this support by editing this registry entry on the client machine before you start a connection.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB

Name: EnableBloombergHID

Type: DWORD

Value: 0 = Disable, 1 = Enable

**Verify support:**

To determine if Bloomberg keyboard support is enabled in Citrix Workspace app, check if the Desktop Viewer correctly reports the Bloomberg keyboard’s devices.

Desktop scenario:
Open the Desktop Viewer. If support for Bloomberg keyboard is enabled, the Desktop Viewer shows see three devices under the USB icon:

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

Seamless Application only scenario:

Open the Connection Center menu from the Citrix Workspace app notification area icon. If support for the Bloomberg keyboard is enabled, the three devices appear in the Devices menu.

The check mark against each of these devices indicates that they are remoted to the session.

Copied!
Failed!

**TWAIN devices**

April 6, 2020

**Requirements**

- The scanner must be TWAIN compliant.
- Install the TWAIN drivers on the local device. They are not required on the server.
- Attach the scanner locally (for example, through USB).
- Ensure that the scanner is using the local TWAIN driver and not the Windows Image Acquisition service.
- Ensure that there is no policy applied to the user account that is used for the test, and which is limiting the bandwidth within the ICA session. For example, client USB redirection bandwidth limit.

For information about policy settings, see [TWAIN devices policy settings](#).

Copied!
Failed!

**Webcams**

August 21, 2020
High definition webcam streaming

Webcams can be used by video conferencing applications running within the virtual session. The application on the server selects the webcam format and resolution based on the supported format types. When a session starts, the client sends the webcam information to the server. Choose a webcam from the video conferencing application. When the webcam and the application both support high-definition rendering, the application uses high-definition resolution. We support webcam resolutions up to 1920x1080.

This feature requires the Citrix Receiver for Windows, minimum version 4.10. For a list of Citrix Workspace app platforms that support HDX webcam redirection, see Citrix Workspace app feature matrix.

For more information about high definition webcam streaming, see HDX video conferencing and webcam video compression.

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 the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

You can use a registry key to disable and enable the feature. The default resolution of 352x288 is used:

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

Name: Enable_HighDefWebcam
Type: REG_DWORD
Data:

0 = Disable the high definition webcam streaming
1 = Enable the high definition webcam streaming

You can use registry keys on the client to configure a specific resolution. Ensure that the camera supports the specified resolution:

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

Name: DefaultWidth
Type: REG_DWORD
Data (decimal): desired width (for example 1280)

Name: DefaultHeight
Type: REG_DWORD
Graphics

April 10, 2020

Citrix HDX graphics include an extensive set of graphics acceleration and encoding technologies that optimize the delivery of rich graphics applications from Citrix Virtual Apps and Desktops. The graphic technologies provide the same experience as using a physical desktop when working remotely with virtual applications that are graphics intensive.

You can use software or hardware for graphics rendering. Software rendering requires a third-party library called software rasterizer. For example, Windows includes the WARP rasterizer for DirectX based graphics. Sometimes, you might want to use an alternative software renderer. Hardware rendering (hardware acceleration) requires a graphics processor (GPU).

HDX Graphics offers a default encoding configuration that is optimized for the most common use cases. By using Citrix policies, IT administrators can also configure various graphics-related settings to meet different requirements and provide the desired user experience.

Thinwire

Thinwire is the Citrix default display remoting technology used in Citrix Virtual Apps and Desktops.

Display remoting technology allows graphics generated on one machine to be transmitted, typically across a network, to another machine for display. Graphics are generated as a result of user input, for example, keystrokes or mouse actions.

HDX 3D Pro

The HDX 3D Pro capabilities in Citrix Virtual Apps and Desktops enable you to deliver desktops and applications that perform best using a graphics processing unit (GPU) for hardware acceleration. These applications include 3D professional graphics applications based on OpenGL and DirectX. The standard VDA supports GPU acceleration of DirectX only.

GPU acceleration for Windows Single-session OS

By using HDX 3D Pro, you can deliver graphically intensive applications as part of hosted desktops or applications on Single-session OS machines. HDX 3D Pro supports physical host computers (including desktop, blade, and rack workstations) and GPU Passthrough and GPU virtualization technologies offered by XenServer, vSphere, and Hyper-V (passthrough only) hypervisors.
Using GPU Passthrough, you can create VMs that have exclusive access to dedicated graphics processing hardware. You can install multiple GPUs on the hypervisor and assign VMs to each of these GPUs on a one-to-one basis.

Using GPU virtualization, multiple virtual machines can directly access the graphics processing power of a single physical GPU.

**GPU acceleration for Windows Multi-session OS**

HDX 3D Pro allows graphics-heavy applications running in Windows Multi-session OS sessions to render on the server graphics processing unit (GPU). By moving OpenGL, DirectX, Direct3D, and Windows Presentation Foundation (WPF) rendering to the server GPU, graphics rendering doesn’t slow down the server CPU. Also, the server is able to process more graphics because the workload is split among the CPU and GPU.

**Framehawk**

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>As of Citrix Virtual Apps and Desktops 7 1903, Framehawk is no longer supported. Instead, use Thinwire with adaptive transport enabled.</td>
</tr>
</tbody>
</table>

Framehawk is a display remoting technology for mobile workers on broadband wireless connections (Wi-Fi and 4G/LTE cellular networks). Framehawk overcomes the challenges of spectral interference and multipath propagation and delivers a fluid and interactive user experience to users of virtual apps and desktops.

**Text-based session watermark**

Text-based session watermarks help to deter and enable tracking data theft. This traceable information appears on the session desktop as a deterrent to those using photographs and screen captures to steal data. You can specify a watermark that is a layer of text. The watermark can display over the entire session screen without changing the content of the original document. Text-based session watermarks require VDA support.

**Related information**

- HDX 3D Pro
- GPU acceleration for Windows Single-session OS
- GPU acceleration for Windows Multi-session OS
- Thinwire
- Text-based session watermark

*Copied!
*Failed!
HDX 3D Pro

July 8, 2020

The HDX 3D Pro capabilities of Citrix Virtual Apps and Desktops enable you to deliver desktops and applications that perform best using a graphics processing unit (GPU) for hardware acceleration. These applications include 3D professional graphics applications based on OpenGL and DirectX. The standard VDA supports GPU acceleration of DirectX only.

For the HDX 3D Pro policy settings, see Optimize for 3D graphics workload.

All supported Citrix Workspace apps can be used with 3D graphics. For best performance with complex 3D workloads, high-resolution monitors, multi-monitor configurations, and high frame rate applications, we recommend the latest versions of Citrix Workspace app for Windows and Citrix Workspace app for Linux. For more information on supported versions of Citrix Workspace app, see Lifecycle Milestones for Citrix Workspace app.

Examples of 3D professional applications include:

- Computer-aided design, manufacturing, and engineering (CAD/CAM/CAE) applications
- Geographical Information System (GIS) software
- Picture Archiving Communication System (PACS) for medical imaging
- Applications using the latest OpenGL, DirectX, NVIDIA CUDA, and OpenCL and WebGL versions
- Computationally intensive non-graphical applications that use NVIDIA Compute Unified Device Architecture (CUDA) GPUs for parallel computing

HDX 3D Pro provides the best user experience over any bandwidth:

- On WAN connections: Deliver an interactive user experience over WAN connections with bandwidths as low as 1.5 Mbps.
- On LAN connections: Deliver a user experience equivalent to that of a local desktop on LAN connections.

You can replace complex and expensive workstations with simpler user devices by moving the graphics processing into the data center for centralized management.

HDX 3D Pro provides GPU acceleration for Windows single-session OS machines and Windows multi-session OS machines. For more information, see GPU acceleration for Windows single-session OS and GPU acceleration for Windows multi-session OS.

HDX 3D Pro is compatible with GPU passthrough and GPU virtualization technologies offered by the following hypervisors, in addition to bare metal:

- Citrix Hypervisor
  - GPU passthrough with NVIDIA GRID, AMD, and Intel GVT-d
Citrix Virtual Apps and Desktops service

- GPU virtualization with NVIDIA GRID, AMD, and Intel GVT-g
- See hardware compatibility at Hypervisor Hardware Compatibility List.

Use the HDX Monitor tool to validate the operation and configuration of HDX visualization technologies and to diagnose and troubleshoot HDX issues. To download the tool and learn more about it, see https://taas.citrix.com/hdx/download/.

**GPU acceleration for Windows multi-session OS**

June 24, 2020

HDX 3D Pro allows graphics-heavy applications running in Windows Multi-session OS sessions to render on the server’s graphics processing unit (GPU). By moving OpenGL, DirectX, Direct3D, and Windows Presentation Foundation (WPF) rendering to the server’s GPU, graphics rendering does not slow the server’s CPU. Also, the server is able to process more graphics because the workload is split between the CPU and GPU.

Since Windows Server is a multi-user operating system, multiple users can share a GPU accessed by Citrix Virtual Apps without the need for GPU virtualization (vGPU).

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

**GPU sharing**

GPU Sharing enables GPU hardware rendering of OpenGL and DirectX applications in remote desktop sessions. It has the following characteristics:

- Can be used on bare metal or virtual machines to increase application scalability and performance.
- Enables multiple concurrent sessions to share GPU resources (most users do not require the rendering performance of a dedicated GPU).
- Requires no special settings.

A GPU can be assigned to the Windows Server virtual machine in either full pass-through or virtual GPU (vGPU) modes following Hypervisor and GPU vendor requirements. Bare-metal deployments on physical Windows Server machines are also supported.
GPU Sharing does not depend on any specific graphics card.

- For virtual machines, select a graphics card that is compatible with the Hypervisor in use. For a Citrix Hypervisor hardware compatibility list, see Hypervisor Hardware Compatibility List.
- When running on bare metal, it is recommended to have a single display adapter enabled by the operating system. If multiple GPUs are installed on the hardware, disable all but one of them using Device Manager.

Scalability using GPU Sharing depends on several factors:

- The applications being run
- The amount of video RAM they consume
- The graphics card’s processing power

Some applications handle video RAM shortages better than others. If the hardware becomes overloaded, instability or a crash of the graphics card driver might occur. Limit the number of concurrent users to avoid such issues.

To confirm that GPU acceleration is occurring, use a third-party tool such as GPU-Z. GPU-Z is available at http://www.techpowerup.com/gpuz/.

- Access to a high-performance video encoder for NVIDIA GPUs and Intel Iris Pro graphics processors. A policy setting (enabled by default) controls this feature and allows the use of hardware encoding for H.264 encoding (where available). If such hardware is not available, the VDA falls back to CPU-based encoding using the software video codec. For more information, see Graphics policy settings.

**DirectX, Direct3D, and WPF rendering**

DirectX, Direct3D, and WPF rendering are only available on servers with a GPU that supports a display driver interface (DDI) version of 9ex, 10, or 11.

- On Windows Server 2008 R2, DirectX and Direct3D require no special settings to use a single GPU.
- On Windows Server 2016 and Windows Server 2012, Remote Desktop Services (RDS) sessions on the RD Session Host server use the Microsoft Basic Render Driver as the default adapter. To use the GPU in RDS sessions on Windows Server 2012, enable the Use the hardware default graphics adapter for all Remote Desktop Services sessions setting in the group policy Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment.
- To enable WPF applications to render using the server’s GPU, create the following settings in the registry of the server running Windows Multi-session OS sessions:
GPU acceleration for CUDA or OpenCL applications

GPU acceleration of CUDA and OpenCL applications running in a user session is disabled by default.

To use the CUDA acceleration POC features, enable the following registry settings:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\Multiple Monitor Hook] “EnableWPFHook”=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_DLLs\Multiple Monitor Hook] “EnableWPFHook”=dword:00000001

To use the OpenCL acceleration POC features, enable the following registry settings:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\Graphics Helper] “CUDA”=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_DLLs\Graphics Helper] “CUDA”=dword:00000001


GPU acceleration for Windows single-session OS

June 25, 2020

With HDX 3D Pro, you can deliver graphically intensive applications as part of hosted desktops or applications on Single-session OS machines. HDX 3D Pro supports physical host computers (including desktop, blade, and rack workstations) and GPU Passthrough and GPU virtualization technologies offered by XenServer, vSphere, and Hyper-V (passthrough only) hypervisors.

HDX 3D Pro offers the following features:

- Adaptive H.264-based or H.265-based deep compression for optimal WAN and wireless performance. HDX 3D Pro uses CPU-based full-screen H.264 compression as the default compression technique for encoding. Hardware encoding with H.264 is used with NVIDIA, Intel, and AMD cards that support NVENC. Hardware encoding with H.265 is used with NVIDIA cards that support NVENC.

- Lossless compression option for specialized use cases. HDX 3D Pro also offers a CPU-based lossless codec to support applications where pixel-perfect graphics are required, such as medical
imaging. True lossless compression is recommended only for specialized use cases because it consumes more network and processing resources.

When using lossless compression:

- The lossless indicator, a notification area icon, notifies the user if the screen displayed is a lossy frame or a lossless frame. This icon helps when the Visual Quality policy setting specifies Build to lossless. The lossless indicator turns green when the frames sent are lossless.

- The lossless switch enables the user to change to Always Lossless mode anytime within the session. To select or deselect Lossless anytime within a session, right-click the icon or use the shortcut ALT+SHIFT+1.

For lossless compression: HDX 3D Pro uses the lossless codec for compression regardless of the codec selected through policy.

For lossy compression: HDX 3D Pro uses the original codec, either the default or the one selected through policy.

Lossless switch settings are not retained for subsequent sessions. To use a lossless codec for every connection, select Always lossless in the Visual quality policy setting.

- You can override the default shortcut, ALT+SHIFT+1, to select or deselect Lossless within a session. Configure a new registry setting at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Name: HKEY_LOCAL_MACHINE_HotKey, Type: String

<table>
<thead>
<tr>
<th>The format to configure a shortcut combination is</th>
<th>1, A=0</th>
<th>1, S=0</th>
<th>1, W=0</th>
<th>1, K=val. Keys must be comma “,” separated. The order of the keys does not matter.</th>
</tr>
</thead>
<tbody>
<tr>
<td>C=0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- A, C, S, W and K are keys, where C=Control, A=ALT, S=SHIFT, W=Win, and K=a valid key. Allowed values for K are 0–9, a–z, and any virtual key code.

- For example:
  * For F10, set K=0x79
  * For Ctrl + F10, set C=1, K=0x79
  * For Alt + A, set A=1, K=a or A=1, K=A or K=A, A=1
  * For Ctrl + Alt + 5, set C=1, A=1, K=5 or A=1, K=5, C=1
* For Ctrl + Shift + F5, set A=1, S=1, K=0x74

**Caution:**

Editing the registry incorrectly can cause serious problems that 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.

- **Multiple and high resolution monitor support.** For Single-session OS machines, HDX 3D Pro supports user devices with up to four monitors. Users can arrange their monitors in any configuration and can mix monitors with different resolutions and orientations. The number of monitors is limited by the capabilities of the host computer GPU, the user device, and the available bandwidth. HDX 3D Pro supports all monitor resolutions and is limited only by the capabilities of the GPU on the host computer.

  HDX 3D Pro also provides limited support for dual-monitor access to Windows XP desktops. For more information about this support, see [VDAs on machines running Windows XP or Windows Vista](#).

- **Dynamic resolution.** You can resize the virtual desktop or application window to any resolution. **Note:** The only supported method to change the resolution is by resizing the VDA session window. Changing resolution from within the VDA session (using Control Panel > Appearance and Personalization > Display > Screen Resolution) is not supported.

- **Support for NVIDIA GRID architecture.** HDX 3D Pro supports NVIDIA GRID cards (see [NVIDIA GRID](#)) for GPU passthrough and GPU sharing. NVIDIA GRID vGPU enables multiple VMs to have simultaneous, direct access to a single physical GPU, using the same NVIDIA graphics drivers that are deployed on non-virtualized operating systems.

- **Support for VMware vSphere and VMware ESX using Virtual Direct Graphics Acceleration (vDGA).** You can use HDX 3D Pro with vDGA for both RDS and VDI workloads.

- **Support for VMware vSphere/ESX using NVIDIA GRID vGPU and AMD MxGPU.**

- **Support for Microsoft HyperV using Discrete Device Assignment in Windows Server 2016.**


- **Support for AMD RapidFire on the AMD FirePro S-series server cards.** HDX 3D Pro supports multi-monitors (up to 6), console blanking, custom resolution, and high frame-rate. Note: HDX 3D Pro support for AMD MxGPU (GPU virtualization) works with VMware vSphere vGPUs only. XenServer and Hyper-V are supported with GPU passthrough. For more information, see [AMD Virtualization Solution](#).
Citrix Virtual Apps and Desktops service

- Access to a high-performance video encoder for NVIDIA GPUs, AMD GPUs, and Intel Iris Pro graphics processors. A policy setting (enabled by default) controls this feature. The feature allows the use of hardware encoding for H.264 encoding (where available). If such hardware is not available, the VDA falls back to CPU-based encoding using the software video codec. For more information, see Graphics policy settings.

As shown in the following figure:

- When a user logs on to Citrix Workspace app and accesses the virtual application or desktop, the Controller authenticates the user. The Controller then contacts the VDA for HDX 3D Pro to broker a connection to the computer hosting the graphical application.

The VDA for HDX 3D Pro uses the appropriate hardware on the host to compress views of the complete desktop or of just the graphical application.

- The desktop or application views and the user interactions with them are transmitted between the host computer and the user device. This transmission is done through a direct HDX connection between Citrix Workspace app and the VDA for HDX 3D Pro.

Install and upgrade NVIDIA drivers
Note:
The NVIDIA GRID API is not the default graphics capture mechanism, but you can enable GRID API for graphics capture. This section applies only when you enable GRID API for graphics capture.

The NVIDIA GRID API provides direct access to the frame buffer of the GPU. This connection provides the fastest possible frame rate for a smooth and interactive user experience. If you install NVIDIA drivers before you install a VDA with HDX 3D Pro, NVIDIA GRID is enabled by default.

To enable NVIDIA GRID on a VM, disable Microsoft Basic Display Adapter from the Device Manager. Run the following command and then restart the VDA:

```
NVFBCEnable.exe -enable -noreset
```

If you install NVIDIA drivers after you install a VDA with HDX 3D Pro, NVIDIA GRID is disabled. Enable NVIDIA GRID by using the NVFBCEnable tool provided by NVIDIA.

To disable NVIDIA GRID, run the following command and then restart the VDA:

```
NVFBCEnable.exe -disable -noreset
```

**Install Intel graphics drivers**

You can install the Intel graphics drivers before installing the VDA. The following step is required if you install Intel drivers after you install a VDA with HDX 3D Pro. The step is also required if the Intel driver has been updated.

To enable the Intel drivers required for multi-monitor support, run the following command using the IntelVirtualDisplayTool.exe, then restart the VDA:

```
IntelVirtualDisplayTool.exe -vd enable
```

IntelVirtualDisplayTool.exe is included with the VDA installer. The IntelVirtualDisplayTool.exe is in `C:\Program Files\Citrix\ICAServices`.

**Optimize the HDX 3D Pro user experience**

To use HDX 3D Pro with multiple monitors, ensure that the host computer is configured with at least as many monitors as are attached to user devices. The monitors attached to the host computer can be either physical or virtual.

Do not attach a monitor (either physical or virtual) to a host computer while a user is connected to the virtual desktop or application providing the graphical application. Doing so can cause instability during a user’s session.

Let your users know that changes to the desktop resolution (by them or an application) are not supported while a graphical application session is running. After closing the application session, a user
can change the resolution of the Desktop Viewer window in the Citrix Workspace app - Desktop Viewer Preferences.

When multiple users share a connection with limited bandwidth (for example, at a branch office), we recommend that you use the **Overall session bandwidth limit** policy setting to limit the bandwidth available to each user. Using this setting ensures that the available bandwidth does not fluctuate widely as users log on and off. Because HDX 3D Pro automatically adjusts to use all the available bandwidth, large variations in the available bandwidth over the course of user sessions can negatively impact performance.

For example, if 20 users share a 60 Mbps connection, the bandwidth available to each user can vary between 3 Mbps and 60 Mbps, depending on the number of concurrent users. To optimize the user experience in this scenario, determine the bandwidth required per user at peak periods and limit users to this amount always.

For users of a 3D mouse, we recommend that you increase the priority of the Generic USB Redirection virtual channel to 0. For information about changing the virtual channel priority, see the Knowledge Center article [CTX128190](https://www.citrix.com/knowledge-center/article/CTX128190).

**Thinwire**

April 7, 2020

**Introduction**

Thinwire, a part of Citrix HDX technology, is the Citrix default display remoting technology used in Citrix Virtual Apps and Desktops.

Display remoting technology allows graphics generated on one machine to be transmitted, typically across a network, to another machine for display.

A successful display remoting solution provides a highly interactive user experience that is similar to that of a local PC. Thinwire achieves this experience by using a range of complex and efficient image analysis and compression techniques. Thinwire maximizes server scalability and consumes less bandwidth than other display remoting technologies.

Because of this balance, Thinwire meets most general business use cases and is used as the default display remoting technology in Citrix Virtual Apps and Desktops.
HDX 3D Pro

In its default configuration, Thinwire can deliver 3D or highly interactive graphics and use a graphics processing unit (GPU), if present. However, we recommend enabling HDX 3D Pro mode using the Optimize for 3D graphics workload or Visual quality > Build to lossless policies for scenarios when GPUs are present. These policies configure Thinwire to use a video codec (H.264 or H.265) to encode the entire screen using hardware acceleration if a GPU is present. Doing so provides a more fluid experience for 3D professional graphics. For more information, see H.264 Build to lossless, HDX 3D Pro, and GPU acceleration for Windows Single-session OS.

Requirements

Thinwire is optimized for modern operating systems, including Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 7, and Windows 10. For Windows Server 2008 R2, legacy graphics mode is recommended. Use the built-in Citrix policy templates, High Server Scalability-Legacy OS and Optimized for WAN-Legacy OS to deliver the Citrix recommended combinations of policy settings for these use cases.

Note:

We do not support legacy graphics mode in this release. It is included for backward compatibility when using XenApp 7.15 LTSR, XenDesktop 7.15 LTSR, and previous VDA releases with Windows 7 and Windows 2008 R2.

- The policy setting which drives the behavior of Thinwire, Use video codec for compression, is available on VDA versions in Citrix Virtual Apps and Desktops 7 1808 or later and XenApp and XenDesktop 7.6 FP3 and later. The Use video codec when preferred option is the default setting on VDA versions Citrix Virtual Apps and Desktops 7 1808 or later and XenApp and XenDesktop 7.9 and later.
- All Citrix Workspace apps support Thinwire. Some Citrix Workspace apps might support features of Thinwire that others do not, for example, 8-bit or 16-bit graphics for reduced bandwidth usage. Support for such features is automatically negotiated by Citrix Workspace app.
- Thinwire uses more server resources (CPU, memory) in multi-monitor and high-resolution scenarios. It is possible to tune the amount of resources Thinwire uses, however, bandwidth usage might increase as a result.
- In low bandwidth or high latency scenarios, consider enabling 8-bit or 16-bit graphics to improve interactivity. Visual quality might be affected, especially at 8-bit color depth.

Encoding methods

Thinwire can operate in two different encoding modes depending on policy and client capabilities:
Citrix Virtual Apps and Desktops service

- Thinwire full screen H.264 or H.265
- Thinwire with selective H.264 or H.265

Legacy GDI remoting uses the XPDM remoting driver and not a Thinwire bitmap encoder.

Configuration

Thinwire is the default display remoting technology.

The following Graphics policy setting sets the default and provides alternatives for different use cases:

- **Use video codec for compression**
  - **Use video codec when preferred.** This is the default setting. No additional configuration is required. Keeping this setting as the default ensures that Thinwire is selected for all Citrix connections, and is optimized for scalability, bandwidth, and superior image quality for typical desktop workloads. This is functionally equivalent to **For actively changing regions**.

- **Other options in this policy setting continue to use Thinwire with other technologies for different use cases.** For example:
  - **For actively changing regions.** The adaptive display technology in Thinwire identifies moving images (video, 3D in motion) and uses H.264 or H.265 only in the part of the screen where the image is moving.
  - **For the entire screen.** Delivers Thinwire with full-screen H.264 or H.265 to optimize for improved user experience and bandwidth in cases with heavy use of 3D graphics. In the case of H.264 4:2:0 (the **Visually lossless** policy is disabled), the final image is not pixel perfect (lossless) and might not be suitable for certain scenarios. In such cases, consider using **H.264 Build to lossless** instead.
Various other policy settings, including the following Visual display policy settings can be used to fine tune the performance of display remoting technology. Thinwire supports them all.

- Preferred color depth for simple graphics
- Target frame rate
- Visual quality

To get the Citrix recommended combinations of policy settings for different business use cases, use the built-in Citrix Policy templates. The **High Server Scalability** and **Very High Definition User Experience** templates both use Thinwire with the optimum combinations of policy settings for your organization's priorities and your users' expectations.

### Monitoring Thinwire

You can monitor the use and performance of Thinwire from Citrix Director. The HDX virtual channel details view contains useful information for troubleshooting and monitoring Thinwire in any session. To view Thinwire-related metrics:

1. In Director, search for a user, machine or endpoint, open an active session and click **Details**. Or, you can select **Filters > Sessions > All Sessions**, open an active session and click **Details**.
2. Scroll down to the **HDX** panel.

3. Select **Graphics - Thinwire**.
Lossless compression codec (MDRLE)

In a typical desktop session, most of the imagery is simple graphics or text regions. Thinwire determines where these regions are and selects these areas for lossless encoding using the 2DRLE codec. At the Citrix Workspace app client side, these elements are decoded using the Citrix Workspace app-side 2DRLE decoder for session display.

In XenApp and XenDesktop 7.17, we added a higher compression ratio MDRLE codec that consumes less bandwidth in typical desktop sessions than the 2DRLE codec. This new codec does not impact server scalability.

Lower bandwidth usually means improved session interactivity (especially on shared or constrained links) and reduced costs. For example, the expected bandwidth consumption when using the MDRLE codec is approximately 10–15% less compared with XenApp and XenDesktop 7.15 LTSR for typical Office-like workloads.

Configuration isn’t required for the MDRLE codec. If Citrix Workspace app supports MDRLE decoding, the VDA uses the VDA MDRLE encoding and the Citrix Workspace app MDRLE decoding. If Citrix Workspace app doesn’t support MDRLE decoding, the VDA automatically falls back to 2DRLE encoding.

MDRLE Requirements:

- Citrix Virtual Apps and Desktops minimum version 7.1808 VDAs
- XenApp and XenDesktop minimum version 7.17 VDAs
- Citrix Workspace app for Windows minimum version 1808
- Citrix Receiver for Windows minimum version 4.11

Progressive Mode

Citrix Virtual Apps and Desktops 1808 introduced progressive mode and enabled it by default. In constrained network conditions (default: bandwidth < 2 Mbps, or latency > 200 ms), Thinwire increased the compression of text and static imagery to improve interactivity during screen activity. The heavily compressed text and images are then progressively sharpened, in a random block fashion, when screen activity stopped. While compressing and sharpening this way improves overall interactivity, it reduces cache efficiency and increases bandwidth usage.

As of Citrix Virtual Apps and Desktops 1906, progressive mode is disabled by default. We now use a different approach. The quality of still images is now based on network conditions and floats between a pre-defined minimum and maximum value for each Visual quality setting. Because there is no explicit sharpening step, Thinwire optimizes image delivery and maintains cache efficiency, while providing nearly all of the benefits of progressive mode.
Changing progressive mode behavior

**Important:**

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.

You can change the progressive mode state with the following registry key:

HKEY_LOCAL_MACHINE\Software\Citrix\Graphics

Type: REG_DWORD

Name: ProgressiveDisplay

Values:

0 = Always off (Disables progressive mode. This value is the default.)
1 = Automatic (Toggle based on network conditions.)
2 = Always on

**H.264 Build to lossless**

**Build to lossless** is a special Thinwire configuration that optimizes graphics delivery for interactivity and final image quality. You can enable this setting by setting the **Visual quality** policy to **Build to lossless**.

Build to lossless compresses the screen using H.264 (or H.265) during screen activity and sharpens to pixel perfect (lossless) when activity stops. The H.264 (or H.265) image quality adapts to available resources to maintain the best possible frame rate. The sharpening step is performed gradually, giving an immediate response if the user begins screen activity shortly after sharpening starts. For example, selecting a model and rotating it.

H.264 **Build to lossless** offers all the advantages of full screen H.264 or H.265, including hardware acceleration, but with the added benefit of a final, guaranteed lossless screen. This is critical for 3D-type workloads that require a final pixel-perfect image. For example, manipulating medical imagery. Also, H.264 **Build to lossless** uses fewer resources than full screen H.264 4:4:4. As a result, using **Build to lossless** usually results in a higher frame rate than Visually lossless H.264 4:4:4.

**Note:**

In addition to the **Visual quality** policy, set the **Use video codec** policy to **Use when preferred** (default) or **For actively changing regions**. You can revert to non-H.264 Build to lossless by setting the **Use video codec** policy to **Do not use video codec**. This results in moving images being...
Text-based session watermark

April 7, 2020

Text-based session watermarks help to deter and enable tracking data theft. This traceable information appears on the session desktop as a deterrent to those using photographs and screen captures to steal data. You can specify a watermark that is a layer of text, which displays over the entire session screen without changing the content of the original document. Text-based session watermarks require VDA support.

Important

Text-based session watermarking is not a security feature. The solution does not prevent data theft completely, but it provides some level of deterrent and traceability. Although we do not guarantee complete information traceability when using this feature, we recommend that you combine this feature with other security solutions as applicable.

The session watermark is text and is applied to the session that is delivered to the user. The session watermark carries information for tracking data theft. The most important data is the identity of the logon user of the current session in which the screen image was taken. To trace the data leakage more effectively, include other information such as server or client internet protocol address and a connect time.

To adjust the user experience, use the Session Watermark policy settings to configure the placement and watermark appearance on the screen.

Requirements:

Virtual Delivery Agents:

Multi-session OS 7.17
Single-session OS 7.17

Limitations:

- Session watermarks are not supported in sessions where Local App Access, Windows media redirection, MediaStream, browser content redirection, and HTML5 video redirection are used. To use session watermark, ensure that these features are disabled.
- Session watermark is not supported and doesn’t appear if the session is running in full-screen hardware accelerated modes (full-screen H.264 or H.265 encoding).
If you set these HDX policies, watermark settings don’t take effect and a watermark isn’t displayed in the session display.

**Use hardware encoding for video codec to Enabled**
**Use video codec for compression to For the entire screen**
- If you set these HDX policies, the behavior is undetermined and the watermark might not display.

**Use hardware encoding for video codec to Enabled**
**Use video codec for compression to Use video codec when preferred**
To ensure the watermark displays, set **Use hardware encoding for video codec to Disabled**, or set **Use video codec for compression to For actively changing regions or Do not use video codec**.

- Session watermark supports only Thinwire and not the Framehawk or Desktop Composition Redirection (DCR) graphic modes.
- If you use Session Recording, the recorded session doesn’t include the watermark.
- If you use Windows remote assistance, the watermark is not shown.
- If a user presses the **Print Screen** key to capture the screen, the screen captured at the VDA side doesn’t include the watermarks. We recommend that you take measures to avoid the captured image being copied.

**Multimedia**

April 7, 2020

The HDX technology stack supports the delivery of multimedia applications through two complementary approaches:

- Server-side rendering multimedia delivery
- Client-side rendering multimedia redirection

This strategy ensures that you can deliver a full range of multimedia formats, with a great user experience, while maximizing server scalability to reduce the cost-per-user.

With server-rendered multimedia delivery, audio and video content is decoded and rendered on the Citrix Virtual Apps and Desktops server by the application. The content is then compressed and delivered using ICA protocol to Citrix Workspace app on the user device. This method provides the highest rate of compatibility with various applications and media formats. Because video processing is
compute-intensive, server-rendered multimedia delivery benefits greatly from the onboard hardware acceleration. For example, support for DirectX Video Acceleration (DXVA) offloads the CPU by performing H.264 decoding in separate hardware. Intel Quick Sync, AMD RapidFire, and NVIDIA NVENC technologies provide hardware-accelerated H.264 encoding.

Because most servers do not offer any hardware acceleration for video compression, server scalability is negatively impacted if all video processing is done on the server CPU. You can maintain high server scalability, by redirecting many multimedia formats to the user device for local rendering.

- Windows Media redirection offloads the server for a wide variety of media formats typically associated with the Windows Media Player.
- HTML5 video has become popular, and Citrix introduced a redirection technology for this type of content. We recommend the browser content redirection for websites using HTML5, HLS, DASH, or WebRTC.
- You can apply the general contact redirection technologies Host-to-client redirection and Local App Access to the multimedia content.

Putting these technologies together, if you don’t configure redirection, HDX does Server-Side Rendering.
If you configure redirection, HDX uses either Server Fetch and Client Render or Client Fetch and Client Render. If those methods fail, HDX falls back to Server-Side Rendering as needed and is subject to the Fallback Prevention Policy.
Example scenarios

Scenario 1. (Server Fetch and Server Rendering):

1. The server fetches the media file from its source, decodes, and then presents the content to an audio device or display device.
2. The server extracts the presented image or sound from the display device or audio device respectively.
3. The server optionally compresses it, and then transmits it to the client.

This approach incurs a high CPU cost, high bandwidth cost (if the extracted image/sound isn’t compressed efficiently), and has low server scalability.

Thinwire and Audio virtual channels handle this approach. The advantage of this approach is that it reduces the hardware and software requirements for the clients. Using this approach the decoding happens on the server and it works for a wider variety of devices and formats.

Scenario 2. (Server Fetch and Client Render):

This approach relies on being able to intercept the media content before it is decoded and presented to the audio or display device. The compressed audio/video content is instead sent to the client where it is then decoded and presented locally. The advantage of this approach is that the are offloaded to the client devices, saving CPU cycles on the server.
Citrix Virtual Apps and Desktops service

However, it also introduces some additional hardware and software requirements for the client. The client must be able to decode each format that it might receive.

**Scenario 3. (Client Fetching and Client Rendering):**

This approach relies on being able to intercept the media content URL before it’s fetched from the source. The URL is sent to the client where the media content is fetched, decoded, and presented locally. This approach is conceptually simple. Its advantage is that it saves both CPU cycles on the server and bandwidth because the server sends only control commands. However, the media content is not always accessible to the clients.

**Framework and platform:**

Single-session operating systems (Windows, Mac OS X, and Linux) provide multimedia frameworks that enable the faster development of multimedia applications. This table lists some of the more popular multimedia frameworks. Each framework divides media processing into several stages and uses a pipelined-based architecture.

<table>
<thead>
<tr>
<th>Framework</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectShow</td>
<td>Windows (98 and later)</td>
</tr>
<tr>
<td>Media Foundation</td>
<td>Windows (Vista and later)</td>
</tr>
<tr>
<td>Gstreamer</td>
<td>Linux</td>
</tr>
<tr>
<td>Quicktime</td>
<td>Mac OS X</td>
</tr>
</tbody>
</table>

**Double hop support with media redirection technologies**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio redirection</td>
<td>No</td>
</tr>
<tr>
<td>Browser content redirection</td>
<td>No</td>
</tr>
<tr>
<td>HDX webcam redirection</td>
<td>Yes</td>
</tr>
<tr>
<td>HTML5 Video redirection</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Media redirection</td>
<td>Yes</td>
</tr>
</tbody>
</table>

© 1999-2020 Citrix Systems, Inc. All rights reserved. 327
Audio features

August 21, 2020

You can configure and add the following Citrix policy settings to a policy that optimizes HDX audio features. For usage details plus relationships and dependencies with other policy settings, see Audio policy settings and Bandwidth policy settings and Multi-stream connections policy settings.

Important:

We recommend delivering audio using User Datagram Protocol (UDP) rather than TCP, but UDP audio encryption using DTLS is available only between Citrix Gateway and Citrix Workspace app. Therefore, sometimes it might be preferable to use TCP transport. TCP supports end-to-end TLS encryption from the Virtual Delivery Agent (VDA) to Citrix Workspace app.

Audio quality

In general, higher sound quality consumes more bandwidth and server CPU utilization by sending more audio data to user devices. Sound compression allows you to balance sound quality against overall session performance; use Citrix policy settings to configure the compression levels to apply to sound files.

By default, the Audio quality policy setting is set to High - high definition audio when TCP transport is used. The policy is set to Medium - optimized-for-speech when UDP transport (recommended) is used. The High Definition audio setting provides high fidelity stereo audio, but consumes more bandwidth than other quality settings. Do not use this audio quality for non-optimized voice chat or video chat applications (such as softphones). The reason being that it might introduce latency into the audio path that is not suitable for real-time communications. We recommend the optimized for speech policy setting for real-time audio, regardless of the selected transport protocol.

When the bandwidth is limited, for example satellite or dial-up connections, reducing audio quality to Low consumes the least possible bandwidth. In this situation, create separate policies for users on low-bandwidth connections so that users on high-bandwidth connections are not adversely impacted.

For setting details, see Audio policy settings. Remember to enable Client audio settings on the user device.

Bandwidth guidelines for audio playback and recording:

- High quality (default)
  - Bitrate: ~100 kbps (min 75, max 175 kbps) for playback / ~70 kbps for microphone capture
  - Number of Channels: 2 (Stereo) for playback, 1 (mono) for microphone capture
Citrix Virtual Apps and Desktops service

- Frequency: 44100 Hz
- Bit-depth: 16-bit
- Medium quality (recommended for VoIP)
  - Bitrate: ~16 kbps (min 20, max 40 kbps) for playback, ~16 kbps for microphone capture
  - Number of Channels: 1 (Mono) for both playback and capture
  - Frequency: 16000 Hz (wideband)
  - Bit-depth: 16-bit
- Low quality
  - Bitrate: ~11 kbps (min 10; max 25 kbps) for playback, ~11 kbps for microphone capture
  - Number of Channels: 1 (Mono) for both playback and capture
  - Frequency: 8000 Hz (narrowband)
  - Bit-depth: 16-bit

Client audio redirection

To allow users to receive audio from an application on a server through speakers or other sound devices on the user device, leave the **Client audio redirection** setting at **Allowed**. This is the default.

Client audio redirection mapping puts extra load on the servers and the network. However, prohibiting client audio redirection disables all HDX audio functionality.

For setting details, see [Audio policy settings](#). Remember to enable client audio settings on the user device.

Client microphone redirection

To allow users to record audio using input devices such as microphones on the user device, leave the **Client microphone redirection** setting at its default (Allowed).

For security, user devices alert their users when servers they don’t trust try to access microphones. Users can choose to accept or reject access before using the microphone. Users can disable this alert on Citrix Workspace app.

For setting details, see [Audio policy settings](#). Remember to enable Client audio settings on the user device.

Audio Plug N Play

The Audio Plug N Play policy setting allows or prevents the use of multiple audio devices to record and play sound. This setting is **Enabled** by default. Audio Plug N Play enables audio devices to be recognized. The devices are recognized even if they are not plugged in until after the user session has started.
Citrix Virtual Apps and Desktops service

This setting applies only to Windows Multi-session OS machines.

For setting details, see Audio policy settings.

Audio redirection bandwidth limit and audio redirection bandwidth limit percent

The Audio redirection bandwidth limit policy setting specifies the maximum bandwidth (in kilobits per second) for a playing and recording audio in a session.

The Audio redirection bandwidth limit percent setting specifies the maximum bandwidth for audio redirection as a percentage of the total available bandwidth.

By default, zero (no maximum) is specified for both settings. If both settings are configured, the one with the lowest bandwidth limit is used.

For setting details, see Bandwidth policy settings. Remember to enable Client audio settings on the user device.

Audio over UDP Real-time Transport and Audio UDP port range

By default, Audio over User Datagram Protocol (UDP) Real-time Transport is allowed (when selected at the time of installation). It opens up a UDP port on the server for connections that use Audio over UDP Real-time Transport. If there is network congestion or packet loss, we recommend configuring UDP/RTP for audio to ensure the best possible user experience. For any real time audio such as soft-phone applications, UDP audio is preferred to EDT. UDP allows for packet loss without retransmission, ensuring that no latency is added on connections with high packet loss.

Important

When Citrix Gateway is not in the path, audio data transmitted with UDP is not encrypted. If Citrix Gateway is configured to access Citrix Virtual Apps and Desktops resources, then audio traffic between the endpoint device and Citrix Gateway is secured using DTLS protocol.

The Audio UDP port range specifies the range of port numbers that the VDA uses to exchange audio packet data with the user device.

By default, the range is 16500 through 16509.

For setting details about Audio over UDP Real-time Transport, see Audio policy settings. For details about Audio UDP port range, see Multi-stream connections policy settings. Remember to enable Client audio settings on the user device.
**Audio setting policies for user devices**

1. Load the group policy templates by following [Configuring the Group Policy Object administrative template](#).
2. In the Group Policy Editor, expand **Administrative Templates > Citrix Components > Citrix Workspace > User Experience**.
3. For **Client audio settings**, select **Not Configured**, **Enabled**, or **Disabled**.
   - **Not Configured.** By default, Audio Redirection is enabled using high quality audio or the previously configured custom audio settings.
   - **Enabled.** Enables audio redirection using the selected options.
   - **Disabled.** Disables audio redirection.
4. If you select **Enabled**, choose a sound quality. For UDP audio, use **Medium** (default).
5. For UDP audio only, select **Enable Real-Time Transport** and then set the range of incoming ports to open in the local Windows firewall.
6. To use UDP Audio with Citrix Gateway, select **Allow Real-Time Transport Through gateway**. Configure Citrix Gateway with DTLS. For more information, see [this article](#).

As an Administrator, if you do not have control on endpoint devices to make these changes, use the default.ica attributes from StoreFront to enable UDP Audio. For example, for bring your own devices or home computers.

1. On the StoreFront machine, open C:\inetpub\wwwroot\Citrix\<Store Name>\App_Data\default.ica with an editor such as notepad.
2. Make the following entries under the [Application] section.
   - ; This text enables Real-Time Transport
     
     EnableRtpAudio=true
   - ; This text allows Real-Time Transport Through gateway
     
     EnableUDPThroughGateway=true
   - ; This text sets audio quality to Medium
     
     AudioBandwidthLimit=1
   - ; UDP Port range
     
     RtpAudioLowestPort=16500
     RtpAudioHighestPort=16509

If you enable User Datagram Protocol (UDP) audio by editing default.ica, then UDP audio is enabled for all users who are using that store.
Avoid echo during multimedia conferences

Users in audio or video conferences might hear an echo. Echoes usually occur when speakers and microphones are too close to each other. For that reason, we recommend the use of headsets for audio and video conferences.

HDX provides an echo cancellation option (enabled by default) that minimizes any echo. The effectiveness of echo cancellation is sensitive to the distance between the speakers and the microphone. Ensure that the devices aren’t too close or too far away from each other.

You can change a registry setting to disable echo cancellation.

**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.

1. Using the Registry Editor on the user device, navigate to one of the following:
   - 32-bit computers: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
   - 64-bit computers: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. Change the **Value data** field to FALSE.

Softphones

A softphone is software acting as a phone interface. You use a softphone to make calls over the internet from a computer or other smart device. By using a softphone, you can dial phone numbers and carry out other phone-related functions using a screen.

Citrix Virtual Apps and Desktops support several alternatives for delivering softphones.

- **Control mode.** The hosted softphone controls a physical telephone set. In this mode, no audio traffic goes through the Citrix Virtual Apps and Desktops server.
- **HDX RealTime optimized softphone support (recommended).** The media engine runs on user device, and Voice over Internet Protocol traffic flows peer-to-peer. For examples, see:
  - HDX Optimization for Microsoft Teams
  - HDX RealTime Optimization Pack, which optimizes the delivery of Microsoft Skype for Business
  - Cisco Jabber Softphone for VDI (formerly known as VXME)
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox (formerly known as VDI Communicator)
  - Zoom VDI Plugin
Citrix Virtual Apps and Desktops service

- Genesys PureEngage Cloud
- Nuance Dragon PowerMic dictation device

- **Local App Access.** A Citrix Virtual Apps and Desktops feature that allows an application such as a softphone to run locally on the Windows user device yet appear seamlessly integrated with their virtual/published desktop. This feature offloads all audio processing to the user device. For more information, see Local App Access and URL redirection.

- **HDX RealTime generic softphone support.** Voice over Internet Protocol-over-ICA.

**Generic softphone support**

Generic softphone support, enables you to host an unmodified softphone on XenApp or XenDesktop in the data center. The audio traffic goes over the Citrix ICA protocol (preferably using UDP/RTP) to the user device running the Citrix Workspace app.

Generic softphone support is a feature of HDX RealTime. This approach to softphone delivery is especially useful when:

- An optimized solution for delivering the softphone is not available and the user is not on a Windows device where Local App Access can be used.
- The media engine that is needed for optimized delivery of the softphone isn’t installed on the user device or isn’t available for the operating system version running on the user device. In this scenario, Generic HDX RealTime provides a valuable fallback solution.

There are two softphone delivery considerations using Citrix Virtual Apps and Desktops:

- How the softphone application is delivered to the virtual/published desktop.
- How the audio is delivered to and from the user headset, microphone, and speakers, or USB telephone set.

Citrix Virtual Apps and Desktops include numerous technologies to support generic softphone delivery:

- Optimized-for-Speech codec for fast encode of the real-time audio and bandwidth efficiency.
- Low latency audio stack.
- Server-side jitter buffer to smooth out the audio when the network latency fluctuates.
- Packet tagging (DSCP and WMM) for Quality of Service.
  - DSCP tagging for RTP packets (Layer 3)
  - WMM tagging for Wi-Fi

The Citrix Workspace app versions for Windows, Linux, Chrome, and Mac also are Voice over Internet Protocol capable. Citrix Workspace app for Windows offers these features:

- Client-side jitter buffer - Ensures smooth audio even when the network latency fluctuates.
- Echo cancellation - Allows for greater variation in the distance between microphone and speakers for workers who do not use a headset.
- Audio plug-n-play - Audio devices do not need to be plugged in before starting a session. They can be plugged in at any time.
- Audio device routing - Users can direct ringtone to speakers but the voice path to their headset.
- Multi-stream ICA - Enables flexible Quality of Service-based routing over the network.
- ICA supports four TCP and two UDP streams. One of the UDP streams supports the real-time audio over RTP.

For a summary of Citrix Workspace app capabilities, see Citrix Receiver Feature Matrix.

**System configuration recommendations**

**Client Hardware and Software:**
For optimal audio quality, we recommend the latest version of Citrix Workspace app and a good quality headset that has acoustic echo cancellation (AEC). Citrix Workspace app versions for Windows, Linux, and Mac support Voice over Internet Protocol. Also, Dell Wyse offers Voice over Internet Protocol support for ThinOS (WTOS).

**CPU Considerations:**
Monitor CPU usage on the VDA to determine if it is necessary to assign two virtual CPUs to each virtual machine. Real-time voice and video are data intensive. Configuring two virtual CPUs reduces the thread switching latency. Therefore, we recommend that you configure two vCPUs in a Citrix Virtual Desktops VDI environment.

Having two virtual CPUs does not necessarily mean doubling the number of physical CPUs, because physical CPUs can be shared across sessions.

Citrix Gateway Protocol (CGP), which is used for the Session Reliability feature, also increases CPU consumption. On high-quality network connections, you can disable this feature to reduce CPU consumption on the VDA. Neither of the preceding steps might be necessary on a powerful server.

**UDP Audio:**
Audio over UDP provides excellent tolerance of network congestion and packet loss. We recommend it instead of TCP when available.

**LAN/WAN configuration:**
Proper configuration of the network is critical for good real-time audio quality. Typically, you must configure virtual LANs (VLANs) because excessive broadcast packets can introduce jitter. IPv6-enabled devices might generate many broadcast packets. If IPv6 support is not needed, you can disable IPv6 on those devices. Configure to support Quality of Service.

**Settings for use WAN connections:**
You can use voice chat over LAN and WAN connections. On a WAN connection, audio quality depends on the latency, packet loss, and jitter on the connection. If delivering softphones to users on a WAN connection, we recommend using the NetScaler SD-WAN between the data center and the remote office. Doing so maintains a high Quality of Service. NetScaler SD-WAN supports Multi-Stream ICA,
including UDP. Also, for a single TCP stream, it’s possible to distinguish the priorities of various ICA virtual channels to ensure that high priority real-time audio data receives preferential treatment.

Use Director or the HDX Monitor to validate your HDX configuration.

Remote user connections:
Citrix Gateway supports DTLS to deliver UDP/RTP traffic natively (without encapsulation in TCP). Open firewalls bidirectionally for UDP traffic over Port 443.

Codec selection and bandwidth consumption:
Between the user device and the VDA in the data center, we recommend using the Optimized-for-Speech codec setting, also known as Medium Quality audio. Between the VDA platform and the IP-PBX, the softphone uses whatever codec is configured or negotiated. For example:

- **G711** provides good voice quality but has a bandwidth requirement of from 80 kilobits per second through 100 kilobits per second per call (depending on Network Layer 2 overheads).
- **G729** provides good voice quality and has a low bandwidth requirement of from 30 kilobits per second through 40 kilobits per second per call (depending on Network Layer 2 overheads).

Delivering softphone applications to the virtual desktop
There are two methods by which you can deliver a softphone to the XenDesktop virtual desktop:

- The application can be installed in the virtual desktop image.
- The application can be streamed to the virtual desktop using Microsoft AppV. This approach has manageability advantages because the virtual desktop image is kept uncluttered. After being streamed to the virtual desktop, the application runs in that environment as if it was installed in the usual manner. Not all applications are compatible with App-V.

Delivering audio to and from the user device
Generic HDX RealTime supports two methods of delivering audio to and from the user device:

- **Citrix Audio Virtual Channel.** We generally recommend the Citrix Audio Virtual Channel because it’s designed specifically for audio transport.
- **Generic USB Redirection.** Supports audio devices having buttons or a display (or both), human interface device (HID), if the user device is on a LAN or LAN-like connection back to the Citrix Virtual Apps and Desktops server.

Citrix audio virtual channel
The bidirectional Citrix Audio Virtual Channel (CTXCAM) enables audio to be delivered efficiently over the network. Generic HDX RealTime takes the audio from the user headset or microphone and compresses it. Then, it sends it over ICA to the softphone application on the virtual desktop. Likewise, the audio output of the softphone is compressed and sent in the other direction to the user headset or speakers. This compression is independent of the compression used by the softphone itself (such as G.729 or G.711). It is done using the Optimized-for-Speech codec (Medium Quality). Its characteristics...
Citrix Virtual Apps and Desktops service

are ideal for Voice over Internet Protocol. It features quick encode time, and it consumes only approximately 56 Kilobits per second of network bandwidth (28 Kbps in each direction), peak. This codec must be explicitly selected in the Studio console because it is not the default audio codec. The default is the HD Audio codec (High Quality). This codec is excellent for high fidelity stereo soundtracks but is slower to encode compared to the Optimized-for-Speech codec.

Generic USB Redirection

Citrix Generic USB Redirection technology (CTXGUSB virtual channel) provides a generic means of remoting USB devices, including composite devices (audio plus HID) and isochronous USB devices. This approach is limited to LAN-connected users. This reason being that the USB protocol tends to be sensitive to network latency and requires considerable network bandwidth. Isochronous USB redirection works well when using some softphones. This redirection provides excellent voice quality and low latency. However, Citrix Audio Virtual Channel is preferred because it is optimized for audio traffic. The primary exception is when you’re using an audio device with buttons. For example, a USB telephone attached to the user device that is LAN-connected to the data center. In this case, Generic USB Redirection supports buttons on the phone set or headset that control features by sending a signal back to the softphone. There isn’t an issue with buttons that work locally on the device.

Limitation

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.

You install an audio device on your client, enable the audio redirection, and start an RDS session. The audio files might fail to play and an error message appears.

As a workaround, add this registry key on the RDS machine, and then restart the machine:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig

Name: EnableSvchostMitigationPolicy

Type: REG_DWORD

Data: 0

Copied!

Failed!
Browser content redirection

August 21, 2020

Browser content redirection prevents the rendering of whitelisted webpages on the VDA side. This feature uses Citrix Workspace app to instantiate a corresponding rendering engine on the client side, which fetches the HTTP and HTTPS content from the URL.

Note:
You can specify that webpages be redirected to the VDA side (and not redirected on the client side) by using a blacklist.

This overlay web layout engine runs on the endpoint device instead of on the VDA and uses the endpoint CPU, GPU, RAM, and Network.

Only the browser viewport is redirected. The viewport is the rectangular area in your browser where content displays. The viewport doesn’t include things like the Address Bar, Favorites Toolbar, Status Bar. Those items are in the user interface, which are still running on the browser in the VDA.

1. Configure a Studio policy that specifies an Access Control List containing the URLs whitelisted for redirection or the blacklist that disables redirection for specific URL paths. For the browser on the VDA to detect that the URL that the user is navigating to matches the whitelist or does not match a blacklist, a browser extension performs the comparison. The browser extension (BHO) for Internet Explorer 11 is included in the installation media and is installed automatically. For

© 1999-2020 Citrix Systems, Inc. All rights reserved.
Chrome, the browser extension is available in the Chrome Web Store, and you can deploy it using the Group Policies and ADMX files. Chrome extensions are installed on a per-user basis. Updating a golden image to add or remove an extension is not required.

2. If a match is found in the whitelist (for example https://www.mycompany.com/), and there is no match to a URL in the blacklist (for example https://www.mycompany.com/engineering), a virtual channel (CTXCSB) instructs Citrix Workspace app that a redirection is required and relays the URL. Citrix Workspace app then instantiates a local rendering engine and displays the website.

3. Citrix Workspace app then blends back the website into the virtual desktop browser content area seamlessly.

The color of the logo specifies the status of the Chrome extension. It is one of these three colors:

- Green: Active and connected.
- Gray: Not active/idle on the current tab.
- Red: Broken/Not working.

You can debug logging by using Options in the extensions menu.

Here are scenarios of how Citrix Workspace app fetches content:

- **Server fetch and server render**: There is no redirection because you didn't whitelist the site or the redirection failed. We fall back to rendering the webpage on the VDA and use Thinwire to remote the graphics. Use policies to control the fallback behavior. High CPU, RAM, and bandwidth consumption on the VDA.

- **Server fetch and client render**: Citrix Workspace app contacts and fetches content from the web server through the VDA using a virtual channel (CTXPFWD). This option is useful when the
client doesn’t have internet access (for example, thin clients). Low CPU and RAM consumption on the VDA, but bandwidth is consumed on the ICA virtual channel.

There are three modes of operation for this scenario. The term proxy refers to a proxy device that the VDA accesses to gain Internet access.

Which policy option to choose:

- **Explicit Proxy** - If you have a single explicit proxy in your Datacenter.
- **Direct or Transparent** - If you do not have proxies, or if you use transparent proxies.
- **PAC files** - If you rely on PAC files so browsers in the VDA can automatically choose the appropriate proxy server for fetching a specified URL.

- **Client fetch and client render**: Because Citrix Workspace app contacts the web server directly, it requires internet access. This scenario offloads all the network, CPU, and RAM usage from your XenApp and XenDesktop Site.
Redirection scenarios

Fallback mechanism:

There might be times when client redirection fails. For example, if the client machine does not have direct internet access, an error response might go back to the VDA. In such cases, the browser on the VDA can then reload and render the page on the server.

You can suppress server rendering of video elements by using the existing Windows media fallback prevention policy. Set this policy to Play all content only on client or Play only client-accessible content on client. These settings block video elements from playing on the server if there are failures in client redirection. This policy takes effect only when you enable browser content redirection and the Access Control List policy contains the URL that falls back. The URL can’t be in the blacklist policy.

System Requirements:

Windows endpoints:

- Windows 7, 8.x, or 10
- Citrix Workspace app 1808 or later
- Citrix Receiver for Windows 4.10 or later

Linux endpoints:

- Citrix Workspace app 1808 for Linux or later
- Citrix Receiver for Linux 13.9 or later
- Thin client terminals must include WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 and XenApp and XenDesktop 7.15 CU5, 7.18, 7.17, 7.16:

Citrix Virtual Apps and Desktops service

- Browser on the VDA:
  - Google Chrome v66 or higher (Chrome requires Citrix Workspace app 1809 for Windows on the user endpoint, Citrix Virtual Apps and Desktops 7 1808 VDA, and the browser content redirection extension)
  - Internet Explorer 11 and configure these options:
    * Clear Enhanced Protected Mode under: Internet Options > Advanced > Security
    * Check Enable third-party browser extensions under: Internet Options > Advanced > Browsing

Troubleshooting

For troubleshooting information, see the Knowledge Center article https://support.citrix.com/article/CTX230052

Browser content redirection Chrome extension

To use browser content redirection with Chrome, add the browser content redirection extension from the Chrome Web Store. Click Add to Chrome in the Citrix Virtual App and Desktop environment.

Important

The extension is not required on the user’s client machine – only in the VDA.

System requirements

- Chrome v66 or higher
- Browser content redirection extension
- Citrix Virtual Apps and Desktops 7 1808 or higher
- Citrix Workspace app 1809 for Windows or higher
This method works for individual users. To deploy the extension to a large group of users in your organization, deploy the extension using Group Policy.

**Deploy the extension using Group Policy**

1. Import the Google Chrome ADMX files into your environment. For information about downloading policy templates and installing and configuring the templates into your Group Policy Editor, see [https://support.google.com/chrome/a/answer/187202?hl=en](https://support.google.com/chrome/a/answer/187202?hl=en).

2. Open your Group Policy Management console and go to **User Configuration \ Administrative Templates\Classic Administrative Templates (ADM) \ Google\ Google Chrome \ Extensions**. Enable the **Configure the list of force-installed apps and extensions** setting.
3. Click **Show** and type the following string, which corresponds to the extension ID. Update the URL for the browser content redirection extension.

```
hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
```
4. Apply the setting and after a `gpupdate` refresh, the user automatically receives the extension. If you launch the Chrome browser in the user’s session, the extension is already applied and they cannot remove it.

Any updates to the extension are automatically installed on the users’ machines through the update URL that you specified in the setting.

If the **Configure the list of force-installed apps and extensions** setting is set to **Disabled**, the extension is automatically removed from Chrome for all users.

**Browser content redirection Edge Chromium extension**

To install the browser content redirection extension in Edge, make sure you have version **83.0.478.37** or higher of the Edge browser installed.

1. Click the **Extensions** option in the menu and turn on **Allow extensions from other stores**.
2. Click the **Chrome Web Store** link and the extension appears at the bar on the top right. For more info on Microsoft Edge extensions, see **Extensions**.

![Chrome Web Store](image)

**Browser content redirection and DPI**

**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.

When using browser content redirection with the DPI (scaling) set to anything over 100% on the user’s machine, the redirected browser content screen displays incorrectly. To avoid this issue, do not set the DPI when using browser content redirection. Another way to avoid the issue is by disabling browser content redirection GPU acceleration for Chrome by creating the following register key on the user’s machine:

```plaintext
\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
```

- **Name**: GPU
- **Type**: DWORD
- **Data**: 0

**HDX video conferencing and webcam video compression**

August 24, 2020
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.

Webcams can be used by applications running within the virtual session by using HDX webcam video compression or HDX plug-n-play generic USB redirection. Use Citrix Workspace app > Preferences > Devices to switch between modes.

Citrix recommends you always use HDX webcam video compression if possible.

To prevent users from switching from HDX webcam video compression, disable USB device redirection by using the policy settings under ICA policy settings > USB Devices policy settings. Citrix Workspace app users can override the default behavior by choosing the Desktop Viewer Mic & Webcam setting Don’t use my microphone or webcam.

HDX webcam video compression

HDX webcam video compression is also called Optimized webcam mode. This type of webcam video compression uses the multimedia framework technology that is part of the client operating system to intercept video from capture devices and transcode and compress it. Manufacturers of capture devices supply drivers that plug into the OS kernel streaming architecture.

The client handles communication with the webcam. The client then sends the video only to the server that can display it properly. The server doesn’t deal directly with the webcam, but it’s integrated giving you the same experience in your desktop. Workspace app compresses the video to save bandwidth and provide better resiliency on WAN scenarios.

HDX webcam video compression requires that the following policy settings be enabled (all are enabled by default).

- Multimedia conferencing
- Windows Media Redirection
Citrix Virtual Apps and Desktops service

If a webcam supports hardware encoding, HDX video compression uses the hardware encoding by default. Hardware encoding might consume more bandwidth than software encoding. To force software compression, add the following DWORD key value to the registry key:

HKEY_CURRENT_USER\Software\Citrix\HdxRealTime:
DeepCompress_ForceSWEncode=1

HDX webcam video compression requirements

Supported clients: Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Workspace app for Chrome, and Citrix Workspace app for Linux.

Note:
Only Citrix Workspace app for Windows, Citrix Workspace app for Chrome, and Citrix Workspace app for Mac 2006 or later support webcam redirection for 64-bit apps.

Supported video conferencing applications (32 bit and 64 bit):

- Adobe Connect
- Cisco Webex and Webex for Teams
- GoToMeeting
- Google Hangouts and Hangouts Meet
- IBM Sametime
- Microsoft Skype for Business 2015
- Microsoft Lync 2010 and 2013
- Microsoft Skype 7 or higher
- Media Foundation-based video applications on Windows 8.x or higher and Windows Server 2012 R2 and higher

To use Skype on a Windows client, edit the registry on the client and the server:

- Client registry key HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
  Name: DefaultHeight
  Type: REG_DWORD
  Data: 240
  Name: DefaultWidth, Type: REG_DWORD
  Data: 320
- Server registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility
  Name: skype.exe,
  Type: REG_DWORD
Citrix Virtual Apps and Desktops service

Data: Set to 0

Other user device requirements:

- Appropriate hardware to produce sound.
- DirectShow-compatible webcam (use the webcam default settings). Webcams that are hardware encoding capable reduces client-side CPU usage.
- For HDX webcam video compression, install webcam drivers on the client, obtained from the camera manufacturer, if possible.

**High definition webcam streaming**

The video conferencing application on the server selects the webcam format and resolution based on the supported format types. When a session starts, the client sends the webcam information to the server. Choose a webcam from the application. When the webcam and the application support high definition rendering, the application uses high definition resolution. We support webcam resolutions up to 1920x1080.

This feature requires the Citrix Workspace app for Windows, minimum version 1808 or Citrix Receiver for Windows, minimum version 4.10.

You can use a registry key to disable and enable the feature. The default resolution of 352x288 is used:

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

Name: Enable_HighDefWebcam

Type: REG_DWORD

Data:

0 = Disable the high definition webcam streaming
1 = Enable the high definition webcam streaming

You can use registry keys on the client to configure a specific resolution. Ensure that the camera supports the specified resolution:

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

Name: DefaultWidth

Type: REG_DWORD

Data (decimal): desired width (for example 1280)

Name: DefaultHeight

Type: REG_DWORD

Data (decimal): desired height (for example 720)
HDX plug-n-play generic USB redirection

HDX plug-n-play generic USB redirection (isochronous) is also called Generic webcam mode. The benefit of HDX Plug-n-Play Generic USB Redirection is that you don’t have to install drivers on your thin client/endpoint. The USB stack is virtualized such that anything you plug into the local client is sent to the remote VM. The remote desktop acts as if you plugged it natively. The Windows desktop handles all the interaction with the hardware and runs through the plug-n-play logic to find the correct drivers. Most webcams work if the drivers exist and can work over ICA. Generic webcam mode uses significantly more bandwidth (many Megabits per second) because you are sending uncompressed video down with USB protocol over the network.

HTML5 multimedia redirection

August 21, 2020

HTML5 multimedia redirection extends the multimedia redirection features of HDX MediaStream to include HTML5 audio and video. Because of growth in online distribution of multimedia content, especially to mobile devices, the browser industry has developed more efficient ways to present audio and video.

Flash has been the standard, but it requires a plug-in, doesn’t work on all devices, and has higher battery usage in mobile devices. Companies like YouTube, Netflix.com, and newer browsers versions of Mozilla, Google, and Microsoft are moving to HTML5 making it the new standard.

HTML5-based multimedia has many advantages over proprietary plug-ins, including:

- Company-independent standards (W3C)
- Simplified digital rights management (DRM) workflow
- Better performance without the security issues raised by plug-ins

HTTP progressive downloads

HTTP progressive download is an HTTP-based pseudo-streaming method that supports HTML5. In a progressive download, the browser plays back a single file (encoded at a single quality) while it is being downloaded from an HTTP web server. The video is stored on the drive as it’s received and is played from the drive. If you rewatch the video, the browser can load the video from cache.
Citrix Virtual Apps and Desktops service

For an example of a progressive download, see the HTML5 video redirection test page. To inspect the video elements in the webpage and find the sources (mp4 container format) in HTML5 video tags, use the developer tools in your browser:

**Comparing HTML5 and Flash**

<table>
<thead>
<tr>
<th>Feature</th>
<th>HTML5</th>
<th>Flash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires a proprietary player</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Runs on mobile devices</td>
<td>Yes</td>
<td>Some</td>
</tr>
<tr>
<td>Running speed on different platforms</td>
<td>High</td>
<td>Slow</td>
</tr>
<tr>
<td>Supported by iOS</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Resource usage</td>
<td>Less</td>
<td>More</td>
</tr>
<tr>
<td>Load faster</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Requirements**

We support only redirection for progressive downloads in mp4 format. We don’t support WebM and Adaptive bitrate streaming technologies like DASH/HLS.

We support the following, and use policies to control them. For more information, see Multimedia policy settings.

- Server side render
- Server fetch client render
- Client side fetching and rendering

Minimum versions of Citrix Workspace app and Citrix Receiver:

- Citrix Workspace app 1808 for Windows
- Citrix Receiver for Windows 4.5
- Citrix Workspace app 1808 for Linux
- Citrix Receiver for Linux 13.5

<table>
<thead>
<tr>
<th>Minimum VDA browser version</th>
<th>Windows OS version/build/SP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 11.0</td>
<td>Windows 10 x86 (1607 RS1) and x64 (1607 RS1); Windows 7 x86 and x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2</td>
</tr>
</tbody>
</table>
Components of the HTML5 video redirection solution


- **WebSocket SSL Certificates**
  - For the CA (root): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
    Location: Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates.
  - For the end-entity (leaf): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
    Location: Certificates (Local Computer) > Personal > Certificates.

- **WebSocketService.exe** - Runs on the local system and performs SSL termination and user session mapping. TLS Secure WebSocket listening on 127.0.0.1 port 9001.

- **WebSocketAgent.exe** - Runs on the user session and renders the video as instructed from WebSocketService commands.

How do I enable HTML5 video redirection?

In this release, this feature is available for controlled webpages only. It requires the addition of the HdxVideo.js JavaScript (included in the Citrix Virtual Apps and Desktops Installation media) to the webpages where the HTML5 multimedia content is available. For example, videos on an internal training site.
Websites like youtube.com, which are based on Adaptive Bitrate technologies (for example, HTTP Live Streaming (HLS) and Dynamic Adaptive Streaming over HTTP (DASH)), are not supported.

For more information, see *Multimedia policy settings*.

**Troubleshooting Tips**

Errors might occur when the webpage tries to run HdxVideo.js. If the JavaScript fails to load, the HTML5 redirection mechanism fails. Ensure that there are no errors related to HdxVideo.js by inspecting the console in the developers tool windows of your browser. For example:

```
[Library.js] webkitExtFullscreen - Found!

Copied!
Failed!
```

**Optimization for Microsoft Teams**

**August 14, 2020**

**Important:**

Optimization for Microsoft Teams requires a minimum of Microsoft Teams version 1.2.00.31357.

Citrix delivers optimization for desktop-based Microsoft Teams using Citrix Virtual Apps and Desktops and Citrix Workspace app. By default, we bundle all the necessary components into the Citrix Workspace app and the Virtual Delivery Agent (VDA).

Our optimization for Microsoft Teams contains VDA-side HDX services and API to interface with the Microsoft Teams hosted app to receive commands. These components open a control virtual channel (CTXMTOP) to the Citrix Workspace app-side media engine. The endpoint decodes and renders the multimedia locally. Reverse seamless snaps-in the local Citrix Workspace app window back into the hosted Microsoft Teams app.

Authentication and signaling occurs natively on the Microsoft Teams-hosted app, just like the other Microsoft Teams services (for example chat or collaboration). Audio/video redirection doesn’t affect them.

**CTXMTOP** is a command and control virtual channel. That means that media is not exchanged between the Citrix Workspace app and the VDA.
Only Client-fetch/client-render is available.

This video demo gives you an idea of how Microsoft Teams works in a Citrix virtual environment.

Microsoft Teams installation

Note:

We recommend installing the VDA before installing Teams in the golden image. This installation order is necessary for the `ALLUSER=1` flag to take effect. If the virtual machine had Teams installed before the VDA was installed, uninstall and reinstall Teams. If you are using App Layering, see the App Layering instructions at the end of this section for more details.

We recommend you follow the Microsoft Teams machine-wide installation guidelines and avoid using the .exe installer that installs Teams in AppData. Instead, install in `C:\Program Files (x86)\Microsoft\Teams` by using the `ALLUSER=1` flag from the command line.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

This example also uses the `ALLUSERS=1` parameter. When you set this parameter, the Teams Machine-Wide Installer appears in Programs and Features in the Control Panel and in Apps & features in Windows Settings for all users of the computer. All users can then uninstall Teams if they have administrator credentials. It’s important to understand the difference between `ALLUSERS=1` and `ALLUSER=1`. You can use the `ALLUSERS=1` parameter in non-VDI and VDI environments. Use the `ALLUSER=1` parameter only in VDI environments to specify a per-machine installation.

In `ALLUSER=1` mode, the Teams application doesn’t auto-update whenever there is a new version. We recommend this mode for non-persistent environments. For example, hosted shared apps or desk-
Citrix Virtual Apps and Desktops service

tops out of a Windows Server or Windows 10 random/pooled catalogs. For more information, see Install Microsoft Teams using MSI (VDI Installation section).

You have Windows 10 dedicated persistent VDI environments. You want the Teams application to auto-update and would prefer Teams to install per-user under Appdata/Local, use the .exe installer or the MSI without ALLUSER=1.

For App Layering:

**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.

Create an empty registry key named PortICA (leave the default Name, Type, and Data).

If using Citrix App Layering to manage VDA and Microsoft Teams installations in different layers, deploy this registry key on Windows before installing Teams with ALLUSER=1:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix

Or

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix

Profile Management recommendations

We recommend using the machine-wide installer for Windows Server and Pooled VDI Windows 10 environments.

When the ALLUSER=1 flag is passed to the MSI from the command line (the machine-wide installer), the Teams app installs under C:\Program Files (x86) (~300 MB). The app uses AppData\Local\Microsoft\TeamsMeetingAddin for logs and AppData\Roaming\Microsoft\Teams (~600–700 MB) for user specific configurations, caching of elements in the user interface, and so forth.

Machine wide installer

The following is an example of folders, desktop shortcuts, and registries created by installing Teams machine-wide installer on a Windows Server 2016 64-bit VM:

*Folder:*

- C:\Program Files (x86)\Microsoft\Teams
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams
Citrix Virtual Apps and Desktops service

**Desktop Shortcut:**

C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe

**Registry:**

- HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run

**Recommendations**

- We recommend disabling auto-start by deleting the Teams registry keys. Doing so prevents “8AM logon storms” from spiking up the VM’s CPU.
- If the Virtual Desktop does not have a GPU/vGPU, we recommend setting **Disable GPU hardware acceleration** in the Teams Settings to improve performance. This setting ("disableGpu":true) is stored in %Appdata%\Microsoft\Teams inside the desktop-config.json file. You can use a logon script to edit that file and set the value to true.
- If using Citrix Workspace Environment Management (WEM), enable **CPU Spikes Protection** to manage processor consumption for Teams.

**Important:**

If you don’t pass the **ALLUSER=1** flag, the MSI places the Teams.exe installer and setup.json under C:\Program Files (x86)\Teams Installer.

A registry key (TeamsMachineInstaller) is added under:

HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run

A subsequent user logon triggers the final installation in **AppData** instead.

**Per-user installer**

When using the .exe installer, the installation process changes significantly, and all the files are placed in AppData.

**Folder:**

- C:\Users\<username>\AppData\Local\Microsoft\Teams
- C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin
- C:\Users\<username>\AppData\Local\SquirrelTemp
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams
Desktop Shortcut:

C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"

Registry:

HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Best Practices

The best practice recommendations are based on the use case scenarios. Using Teams with a non-persistent setup requires a profile caching manager for efficient Teams runtime data synchronization. Having a profile caching manager ensures that the appropriate user-specific information (for example, user data, profile, and settings) is cached during the user session. Make sure you synchronize the data in these two folders:

- C:\Users\<username>\AppData\Local\Microsoft\IdentityCache
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

Teams cached content exclusion list for non-persistent setup:

Exclude the following items from the Teams caching folder, %AppData%/Microsoft/Teams. Excluding these items helps reduce the user caching size to further optimize your non-persistent setup.

Exclusion list – directories

- Roaming\Microsoft\Teams*.txt
- Roaming\Microsoft\Teams\media-stack
- Roaming\Microsoft\Teams\Service Worker\CacheStorage
- Roaming\Microsoft\Teams\Logs
- Roaming\Microsoft\Teams\Application Cache
- Roaming\Microsoft\Teams\Cache
- Roaming\Microsoft\Teams\GPUCache
- Roaming\Microsoft\Teams\meeting-addin\Cache (Critical for issues where the Add-in is missing in Outlook)

Use case: single session scenario:

In this scenario, the end user uses Microsoft Teams in one location at a time. There is no need to run Teams in two different Windows sessions simultaneously. For instance, in a common virtual desktop deployment, each user is assigned to one desktop, Teams is deployed inside the virtual desktop as one application.

We recommend enabling the Citrix Profile container and redirect the previously mentioned per-user directories into the container.

1. Deploy the Microsoft Teams machine wide installer (ALLUSER=1) in the golden image.
2. Enable Citrix Profile Management and set up the user profile store with the proper permissions.

3. Enable the following Profile Management policy setting: **File system > Synchronization > Profile container – List of folders to be contained in profile disk.**

   ![Edit Setting](image)

   List all the previously mentioned folders into this configuration. Alternatively, you can also configure these settings using the Citrix Workspace Environment Management (WEM) service.

4. Apply the settings to the correct Delivery Group.

5. Log in to validate the deployment.

**System requirements**

Minimum recommended version - Delivery Controller (DDCs) 1906.2 (If you’re using an earlier version, see **Enable optimization of Microsoft Teams**):

Supported operating systems:
Citrix Virtual Apps and Desktops service

- Windows Server 2019, 2016, 2012R2 Standard and Datacenter Editions, and with the Server Core option

**Minimum version - Virtual Delivery Agents (VDAs) 1906.2:**

Supported operating systems:

- Windows 10 64-bit, versions 1607 and higher.

Requirements:

- BCR_x64.msi - the MSI that contains the Microsoft Teams optimization code and starts automatically from the GUI. If you’re using the command line interface for the VDA installation, don’t exclude it.

**Recommended version – Citrix Workspace app 2006.1 for Windows and Minimum version - Citrix Workspace app 1907 for Windows:**

- Windows 7, 8, and 10 (32-bit and 64-bit editions, including Embedded editions)
- Windows 10 IoT Enterprise 2016 LTSC (v1607) and 2019 LTSC (v1809)
- Processor (CPU) architectures supported: x86 and x64 (ARM is not supported)
- Endpoint requirement: Approximately 2.2–2.4 GHz dual core CPU that can support 720p HD resolution during a peer-to-peer video conference call.
- Dual or quad-core CPUs with lower base speeds (~1.5 GHz) equipped with Intel Turbo Boost or AMD Turbo Core that can boost up to at least 2.4 GHz.
- HP Thin Clients verified: t630/t640, t730/t740, mt44/mt45.
- Dell Thin Clients verified: 5070, 5470 Mobile TC.
- 10ZiG Thin Clients verified: 4510 and 5810q.
- For a complete list of verified endpoints, see Thin Clients.
- Citrix Workspace app requires a minimum of 600 MB free disk space and 1 GB RAM.
- Microsoft .NET Framework minimum requirement is version 4.6.2. Citrix Workspace app automatically downloads and installs .NET Framework if it is not present in the system.

**Minimum version - Citrix Workspace app 2006 for Linux:**

For more information, see Optimization for Microsoft Teams in What’s new in 2006.

Software:

- GStreamer 1.0 or later or Cairo 2
- libc++-9.0 or later
- libgdk 3.22 or later
- OpenSSL 1.1.1d
- x64 Linux distribution

Hardware:
Citrix Virtual Apps and Desktops service

- Minimum 1.8 GHz dual-core CPU that can support 720p HD resolution during a peer-to-peer video conference call.
- Dual or quad-core CPU with a base speed of 1.8 GHz and a high Intel Turbo Boost speed of at least 2.9 GHz.

For more information, see Prerequisites to install Citrix Workspace app.

Enable optimization of Microsoft Teams

To enable optimization for Microsoft Teams, use the Studio policy described in Microsoft Teams redirection policy (it is ON by default). In addition to this policy being enabled, HDX checks to verify that the version of the Citrix Workspace app is equal to or greater than the minimum required version. If you enabled the policy and the Citrix Workspace app version is supported, the `HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport` registry key is set to 1 automatically on the VDA. The Microsoft Teams application reads the key to load in VDI mode.

Note:

If you are using version 1906.2 VDAs or higher with older Controller versions (for example, version 7.15), which do not have the policy available in Studio, you can still be optimized because HDX optimization for Microsoft Teams is enabled by default in the VDA.

If you click About > Version, the Citrix HDX Optimized legend displays:

If you see Citrix HDX Not Connected instead, the Citrix API is loaded in Teams (which is the first step towards redirection), but there was an error in the subsequent parts of the stack. The error is most likely in the VDA services or the Citrix Workspace app).

If you don’t see any legend, Teams failed to load the Citrix API. Exit Teams by right-clicking on the notification area icon and restart. Make sure the Studio policy is not set to Prohibited, and that the Citrix Workspace app version is supported.

Network requirements

Microsoft Teams relies on Media Processor servers in Office 365 for meetings or multiparty calls. Microsoft Teams relies on Office 365 Transport Relays for these scenarios:
Citrix Virtual Apps and Desktops service

- Two peers in a point-to-point call do not have direct connectivity
- A participant does not have direct connectivity to the media processor.

Therefore, the network health between the peer and the Office 365 cloud determines the performance of the call.

We recommend evaluating your environment to identify any risks and requirements that can influence your overall cloud voice and video deployment.

Use the Skype for Business Network Assessment Tool to test if your network is ready for Microsoft Teams. For support information, see Support.

**Summary of key network recommendations for Real Time Protocol (RTP) traffic:**

- Connect to the Office 365 network as directly as possible from the branch office.
- If you must use any of the following at the branch office, ensure that RTP/UDP Teams traffic is unhindered. HdxTeams.exe doesn’t honor explicit proxies configured on the endpoint.
  - Bypass proxy servers
  - Network SSL intercept
  - Deep packet inspection devices
  - VPN hairpins (use split tunneling if possible)
- Plan and provide sufficient bandwidth.
- Check each branch office for network connectivity and quality.

The WebRTC media engine in the Workspace app (HdxTeams.exe) uses the Secure Real-time Transport Protocol (SRTP) for multimedia streams that are offloaded to the client. SRTP provides confidentiality and authentication to RTP by using symmetric keys (128 bit) to encrypt media and control messages, and uses the AES encryption cipher in counter mode.

The following metrics are recommended for guaranteeing a positive user experience:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Endpoint to Office 365</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latency (one way)</td>
<td>&lt; 50 msec</td>
</tr>
<tr>
<td>Latency (RTT)</td>
<td>&lt; 100 msec</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>&lt;1% during any 15s interval</td>
</tr>
<tr>
<td>Packet inter-arrival jitter</td>
<td>&lt;30ms during any 15s interval</td>
</tr>
</tbody>
</table>

For more information, see Prepare your organization’s network for Microsoft Teams.

In terms of bandwidth requirements, optimization for Microsoft Teams can use a wide variety of codecs for audio (OPUS/G.722/PCM G711) and video (H264/VP9).

The peers negotiate these codecs during the call establishment process using the Session Description Protocol (SDP) Offer/Answer.
Citrix Virtual Apps and Desktops service

Citrix minimum recommendations are:

<table>
<thead>
<tr>
<th>Type</th>
<th>Bandwidth</th>
<th>Codec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio (each way)</td>
<td>~90 kbps</td>
<td>G.722</td>
</tr>
<tr>
<td>Audio (each way)</td>
<td>~60 kbps</td>
<td>Opus*</td>
</tr>
<tr>
<td>Video (each way)</td>
<td>~700 kbps</td>
<td>H264 360p @ 30 fps 16:9</td>
</tr>
<tr>
<td>Video (each way)</td>
<td>~2,500 kbps</td>
<td>VP9 720p @ 30 fps 16:9</td>
</tr>
<tr>
<td>Screen sharing</td>
<td>~300 kbps</td>
<td>H264 1080p @ 15 fps</td>
</tr>
</tbody>
</table>

* Opus supports constant and variable bitrate encoding from 6 kbps up to 510 kbps. Opus and VP9 are the preferred codecs for peer-to-peer calls between two optimized VDI users. G.722 and H264 are the preferred codecs for a VDI user joining a meeting.

**Call establishment and media flow paths**

When possible, the HDX media engine in the Citrix Workspace app (HdxTeams.exe) tries to establish a direct network Secure Real-time Transport Protocol (SRTP) connection over User Datagram Protocol (UDP) in a peer-to-peer call. If the UDP ports are blocked, the media engine falls back to TCP 443.

The HDX media engine supports ICE, Session Traversal Utilities for NAT (STUN), and Traversal Using Relays around NAT (TURN) for candidate discovery and connection establishment.

If there is no direct path between the two peers or between a peer and a conference server (if the user is joining a multi-party call or meeting), HdxTeams.exe uses a Microsoft Teams transport relay server in Office 365 to reach the other peer or the media processor (where meetings are hosted). The user’s client machine must have access to two Office 365 subnet IP address ranges and 4 UDP ports. For more information, see the Architecture diagram in the “Call setup” section further down and Office 365 URLs and IP address ranges ID 11.

<table>
<thead>
<tr>
<th>ID</th>
<th>Category</th>
<th>Addresses</th>
<th>Destination Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Optimize required</td>
<td>13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14</td>
<td><strong>UDP:</strong> 3478, 3479, 3480, 3481, <strong>TCP:</strong> 443 (fallback)</td>
</tr>
</tbody>
</table>

These ranges contain both Transport Relays and media processors. The Teams Transport Relays provide STUN and TURN functionality, but they are not ICE endpoints.
Also, the Teams Transport Relays do not terminate media nor perform any transcoding. They can bridge TCP (if HdxTeams.exe uses TCP) to UDP when they forward traffic to other peers or media processors.

HdxTeams.exe contacts the closest Microsoft Teams Transport Relay in the Office 365 cloud. HdxTeams.exe uses anycast IP and port 3478–3481 UDP (different UDP ports per workload, though multiplexing can happen) or 443 TCP TLSv1.2 for fallbacks. Call quality depends on the underlying network protocol. Because UDP is always recommended over TCP, we advise you to design your networks to accommodate UDP traffic in the branch office.

If Teams loaded in optimized mode and HdxTeams.exe is running on the endpoint, Interactive Connectivity Establishment (ICE) failures might cause a call setup failure or one-way-only audio/video. When a call cannot be completed or media streams are not full duplex, check the Wireshark trace on the endpoint first. For more information about the ICE candidate gathering process, see “Collecting logs” in the Support section.

Note:
If the endpoints don’t have internet access, it might still be possible for the user to make a peer-to-peer call only if they are on the same LAN. Meetings fail. In this case, there is a 30 second timeout before the call setup begins.

Call setup
Use this architecture diagram as a visual reference for the call flow sequence. The corresponding steps are indicated in the diagram.

Architecture:
1. Launch Microsoft Teams.

2. Teams authenticates to O365. Tenant policies are pushed down to the Teams client, and relevant TURN and signaling channel information is relayed to the app.

3. Teams detects that it is running in a VDA and makes API calls to the Citrix JavaScript API.

4. Citrix JavaScript in Teams opens a secure WebSocket connection to WebSocketService.exe running on the VDA (127.0.0.1:9002), which spawns WebSocketAgent.exe inside the user session.

5. WebSocketAgent.exe instantiates a generic virtual channel by calling into the Citrix HDX Teams Redirection Service (CtxSvcHost.exe).
6. Citrix Workspace app's wfica32.exe (HDX engine) spawns a new process called HdxTeams.exe, which is the new WebRTC engine used for Teams optimization.

7. HdxTeams.exe and Teams.exe have a 2-way virtual channel path and can start processing multimedia requests.

--- User calls ---

8. **Peer A** clicks the **call** button. Teams.exe communicates with the Teams services in Office 365 establishing an end-to-end signaling path with **Peer B**. Teams asks HdxTeams for a series of supported call parameters (codecs, resolutions, and so forth, which is known as a Session Description Protocol (SDP) offer). These call parameters are then relayed using the signaling path to the Teams services in Office 365 and from there to the other peer.

9. The SDP offer/answer (single-pass negotiation) takes place through the signaling channel, and the ICE connectivity checks (NAT and Firewall traversal using Session Traversal Utilities for NAT (STUN) bind requests) complete. Then, Secure Real-time Transport Protocol (SRTP) media flows directly between HdxTeams.exe and the other peer (or Office 365 conference servers if it is a meeting).

**Microsoft Phone System**

Phone System is Microsoft’s technology that enables call control and PBX capabilities in the Office 365 cloud with Microsoft Teams. Optimization for Microsoft Teams supports Phone System, using Office 365 Calling Plans or Direct Routing. With Direct Routing, you connect your own supported session border controller to the Microsoft Phone System directly without any additional on-premises software.

**Firewall considerations**

When users initiate an optimized call using the Microsoft Teams client for the first time, they might notice a warning with the **Windows firewall** settings. The warning asks for users to allow communication for HdxTeams.exe (HDX Overlay Teams).
The following four entries are added under **Inbound Rules** in the **Windows Defender Firewall > Advanced Security** console. You can apply more restrictive rules if desired.

**Microsoft Teams and Skype for Business Coexistence**

You can deploy Microsoft Teams and Skype for Business side by side, as two separate solutions with overlapping capabilities. For more information, see [Understand Microsoft Teams and Skype for Business coexistence and interoperability](#).

Citrix RealTime Optimization Pack and HDX optimization for Teams multimedia engines then honor whatever configuration is set in your environment (for example, island modes, Skype for Business with Teams collaboration, Skype for Business with Teams collaboration and meetings).

Peripheral access can be granted only to a single application at the time. For example, webcam access by the RealTime Media Engine during a call locks the imaging device during a call. When the device is released, it becomes available for Teams.
Citrix Virtual Apps and Desktops service

Citrix SD-WAN: optimized network connectivity for Microsoft Teams

Optimal audio and video quality require a network connection to the Office 365 cloud that has low latency, low jitter, and low packet loss. Backhauling of Microsoft Teams audio-video RTP traffic from Citrix Workspace app users at branch office locations to a data center before going to the internet can add excessive latency and might also cause congestion on WAN links. Citrix SD-WAN optimizes connectivity for Microsoft Teams following Microsoft Office 365 network connectivity principles. Citrix SD-WAN uses the Microsoft REST-based Office 365 IP address and web service and proximate DNS to identify, categorize, and steer Microsoft Teams traffic.

Business broadband internet connections in many areas suffer from intermittent packet loss, periods of excessive jitter, and outages.

Citrix SD-WAN offers two solutions to preserve Microsoft Teams audio-video quality when network health is variable or degraded.

- If you use Microsoft Azure, a Citrix SD-WAN virtual appliance (VPX) deployed in the Azure VNET provides advanced connectivity optimizations. These optimizations include seamless link failover and audio packet racing.
- Alternatively, Citrix SD-WAN customers can connect to Office 365 through the Citrix Cloud Direct service. This service provides reliable and secure delivery for all internet-bound traffic.

If the quality of the branch office internet connection is not a concern, it might be sufficient to minimize latency by steering Microsoft Teams traffic directly from the Citrix SD-WAN branch appliance to the nearest Office 365 front door. For more information, see Citrix SD-WAN Office 365 optimization.
**Gallery view and active speakers in Microsoft Teams**

Only a single incoming video stream is supported in meetings or group calls. When there are multiple participants sending their video, only the dominant speaker’s video is shown at any time. There might be one- or two-second delay between the time a speaker is detected as active and the time the video feed displays.

**Screen sharing in Microsoft Teams**

Microsoft Teams relies on video-based screen sharing (VBSS), effectively encoding the desktop being shared with video codecs like H264 and creating a high-definition stream. With HDX optimization, incoming screen sharing is treated as a video stream. Therefore, if you are in the middle of a video call and the other peer starts to share the desktop, that original camera video feed is paused. Instead, the screen sharing video feed displays. The peer must then manually resume the camera sharing.

Outgoing screen sharing is also optimized and offloaded to the Citrix Workspace app (version 1907 or higher). In this case, HdxTeams.exe captures and transmits only the Citrix Desktop Viewer (CD-Viewer.exe) window. If you want to share a local application running in your client machine, you can overlay it on top of CDViewer and it is also captured.

Multi-monitor: In cases where CDViewer is in full screen mode and spanning across multi-monitor setups, only the primary monitor is shared. Users must drag the application of interest inside the virtual desktop to the primary monitor for the other peer on the call to see it.

![Citrix Desktop Viewer](image)

**Note:**

If you are publishing Teams as a stand-alone seamless application, screen sharing captures the local desktop of your physical endpoint in Citrix Workspace app minimum version 1909.

**Peripherals in Microsoft Teams**

When optimization for Microsoft Teams is active, the Citrix Workspace app accesses the peripherals (headset, microphone, cameras, speakers, and so forth). Then the peripherals are properly enumer-
Citrix Virtual Apps and Desktops service

ated in the Microsoft Teams UI (Settings > Devices).

Microsoft Teams does not access the devices directly. Instead, it relies on HdxTeams.exe for acquiring, capturing, and processing the media. Microsoft Teams lists the devices for the user to select.

Recommendations:

- Microsoft Teams certified headsets with built-in echo cancellation. In setups with multiple peripherals, where microphone and speakers are on separate devices an echo might be present. For example, a webcam with a built-in microphone, and a monitor with speakers. When using external speakers, place them as far as possible from the microphone and from any surface that might refract the sound into the microphone.
- Microsoft Teams certified cameras, although Skype for Business certified peripherals are compatible with Microsoft Teams.
- HdxTeams.exe cannot take advantage of CPU offloading with webcams that perform on-board H.264 encoding -UVC 1.1 and 1.5.

Note:

HdxTeams.exe supports only these specific audio device formats (channels, bit depth, and sample rate):

- Playback Devices: up to 2 channels, 16 bit, frequencies up to 96,000 Hz
- Recording Devices: up to 4 channels, 16 bit, frequencies up to 96,000 Hz

Even if one speaker or microphone does not match the expected settings, device enumeration in Teams fails and None displays under Settings > Devices.

Webrtc logs in HdxTeams.exe show this type of information:

Mar 27 20:58:22.885 webrtcapi.WebRTC Engine Info: init. initializing...

As a workaround, open the Sound Control Panel (mmsys.cpl), select the playback or recording device, go to Properties > Advanced and change the settings to a supported mode. Alternatively, disable the specific device.

**Fallback mode**

If Microsoft Teams fails to load in optimized VDI mode, the VDA uses legacy HDX technologies like Webcam redirection and client audio and microphone redirection. In the unoptimized mode, the peripherals are mapped to the VDA. The peripherals appear to the Microsoft Teams app as if they were locally attached to the virtual desktop.

To determine if you are in optimized or unoptimized mode when looking at the **Settings > Devices** tab in Teams, the most significant difference is the camera name. If Microsoft Teams loaded in unoptimized mode, legacy HDX technologies launch. The webcam name has the **Citrix HDX** suffix as shown in the following graphic. The speaker and microphone device names might be slightly different (or truncated) when compared to the optimized mode.

When legacy HDX technologies are used, Microsoft Teams doesn’t offload audio, video, and screen sharing processing to the endpoint’s Citrix Workspace app WebRTC media engine. Instead, HDX technologies use server-side rendering. Expect high CPU consumption on the VDA when you turn on video. Real time audio performance might not be optimal.

© 1999-2020 Citrix Systems, Inc. All rights reserved.
## Known limitations

<table>
<thead>
<tr>
<th>Limitations</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pop out chat is not supported.</td>
<td>Citrix and Microsoft limitation</td>
</tr>
<tr>
<td>Gallery view - Active speaker only.</td>
<td>Teams dependency – Contact Microsoft for when to expect Gallery View (2x2)</td>
</tr>
<tr>
<td>HID buttons - Answer and end call not supported. Volume up and down are</td>
<td>Citrix Workspace app limitation</td>
</tr>
<tr>
<td>supported.</td>
<td></td>
</tr>
<tr>
<td>When switching the peripheral input or output in <strong>Settings &gt; Devices</strong> in</td>
<td>you might experience a one second audio glitch.</td>
</tr>
<tr>
<td>the middle of the call, you might experience a one second audio glitch.</td>
<td></td>
</tr>
<tr>
<td>When doing screen sharing in multi-monitor setups, only the main monitor</td>
<td>Citrix Workspace app limitation</td>
</tr>
<tr>
<td>is shared.</td>
<td></td>
</tr>
<tr>
<td>When you configure the Citrix Workspace app High DPI setting to **No, use the native resolution, the redirected video window appears out place when the monitor’s DPI scaling factor is set to anything above 100%.</td>
<td>Citrix Workspace app limitation</td>
</tr>
<tr>
<td>We don’t support Dual Tone Multi Frequency (DTMF) interaction with telephony systems.</td>
<td>Citrix Workspace app limitation</td>
</tr>
<tr>
<td>When doing screen sharing, the option <strong>include system audio</strong> is not available.</td>
<td>Citrix and Microsoft limitation</td>
</tr>
<tr>
<td>Interoperability with Skype for Business is limited to audio calls, no video modality.</td>
<td>Microsoft limitation</td>
</tr>
<tr>
<td>Incoming and outgoing video stream maximum resolution is 720p.</td>
<td>Teams dependency – contact Microsoft for when to expect 1080p</td>
</tr>
<tr>
<td>We support only one video stream from an incoming camera or screen share stream.</td>
<td>Teams dependency – contact Microsoft</td>
</tr>
<tr>
<td>When there’s an incoming screen share, that screen share is shown it instead of the video of the dominant speaker.</td>
<td></td>
</tr>
<tr>
<td>Outgoing screen sharing: Application sharing is not supported.</td>
<td>Citrix Workspace app and VDA limitation</td>
</tr>
<tr>
<td>We don’t support live events.</td>
<td>Citrix and Teams limitation</td>
</tr>
</tbody>
</table>

© 1999-2020 Citrix Systems, Inc. All rights reserved.
## Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Limitations</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Give control and take control: Not supported during a screen sharing or application sharing session and supported during a PowerPoint sharing session.</td>
<td>Teams dependency – contact Microsoft</td>
</tr>
<tr>
<td>In outgoing screen sharing, the mouse pointer is not captured</td>
<td>Citrix limitation</td>
</tr>
<tr>
<td>Secondary ringer <em>(Teams &gt; Settings &gt; Devices)</em> is not supported</td>
<td>Citrix limitation</td>
</tr>
<tr>
<td>During a call, if a user opens a file shared through Microsoft Teams, the call might disconnect.</td>
<td>Microsoft limitation</td>
</tr>
<tr>
<td>PSTN call ringback tone is not supported</td>
<td>Teams dependency – Contact Microsoft</td>
</tr>
<tr>
<td>The Call Quality Dashboard for Microsoft Teams does not display data for VDI users</td>
<td>Teams limitation – Contact Microsoft</td>
</tr>
</tbody>
</table>

### Additional information

- Monitor, troubleshoot, and support Microsoft Teams
- Deploy the Teams desktop app to the VM
- Install Microsoft Teams using MSI (VDI Installation section)
- Thin clients
- Skype for Business Network Assessment Tool
- Understand Microsoft Teams and Skype for Business coexistence and interoperability

*Copied!*
*Failed!*

## Monitor, troubleshoot, and support Microsoft Teams

### August 21, 2020

### Monitor Teams

This section provides guidelines for monitoring Microsoft Teams optimization with HDX.
If the user is running in optimized mode and `HdxTeams.exe` is running on the client machine, there is
Citrix Virtual Apps and Desktops service

a process in the VDA called WebSocketAgent.exe running in the session. Use the Activity Manager in Director to see the application.

With the VDA minimum version 1912, you can monitor active Teams calls using the Citrix HDX Monitor (minimum version 3.11). The Citrix Virtual Apps and Desktops product ISO contains the latest hdxmonitor.msi in the folder layout\image-full\Support\HDX Monitor.

For more information, see Monitoring in the Knowledge Center article CTX253754.

Troubleshoot

This section provides troubleshooting tips for issues that you might encounter when using optimization for Microsoft Teams. For more information, see CTX253754.

On the Virtual Delivery Agent

There are four services installed by BCR_x64.msi. Only two are responsible for Microsoft Teams redirection in the VDA.

- **Citrix HDX Teams Redirection Service** establishes the virtual channel used in Microsoft Teams. The service relies on CtxSvcHost.exe.
Citrix HDX HTML5 Video Redirection Service runs as WebSocketService.exe listening on 127.0.0.1:9002 TCP. WebSocketService.exe performs two main functions:

i. **TLS termination for secure WebSockets** receives a secure WebSocket connection from vdiCitrixPeerConnection.js, which is a component inside the Microsoft Teams app. You can track it with the Process Monitor. For more information about certificates, see the section “TLS and HTML5 video redirection, and browser content redirection” under Communication between Controller and VDA.

Some antivirus and desktop security software interferes with the proper functioning of WebSocketService.exe and its certificates. While the Citrix HDX HTML5 Video Redirection service might be running in the services.msc console, the localhost 127.0.0.1:9002 TCP socket is never in listening mode as seen in netstat. Trying to restart the service causes it to hang (“Stopping…”). Ensure you apply the proper exclusions for the WebSocketService.exe process.

ii. **User session mapping.** When the Microsoft Teams application starts, WebSocketService.exe starts the WebSocketAgent.exe process in the user’s session in the VDA. WebSocketService.exe runs in Session 0 as a LocalSystem account.

You can use **netstat** to check if the WebSocketService.exe service is in an active listening state in the VDA.

Run `netstat -anob -p tcp` from an elevated command prompt window:

```
TCP   127.0.0.1:9001     0.0.0.0:0   LISTENING   11740
TCP   127.0.0.1:9002     0.0.0.0:0   LISTENING   11740
```

On a successful connection, the state changes to ESTABLISHED:

```
TCP   127.0.0.1:9002 127.0.0.1:58069 ESTABLISHED 8096
TCP   127.0.0.1:9002 127.0.0.1:9002 ESTABLISHED 748
```

**Important:**

WebSocketService.exe listens in two TCP sockets, 127.0.0.1:9001 and 127.0.0.1:9002. Port 9001
Citrix Virtual Apps and Desktops service

is used for browser content redirection and HTML5 video redirection. Port 9002 is used for Microsoft Teams redirection. Ensure that you don’t have any proxy configurations in the Windows OS of the VDA that can prevent a direct communication between Teams.exe and WebSocketService.exe. Sometimes, when you configure an explicit proxy in Internet Explorer 11 (Internet Options > Connections > LAN settings > Proxy Server), connections might flow through an assigned proxy server. Verify that Bypass proxy server for local addresses is checked when using a manual and explicit proxy setting.

Services locations and descriptions

<table>
<thead>
<tr>
<th>Service</th>
<th>Path to executable in Windows Server OS</th>
<th>Log on as</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix HTML5 Video Redirection Service</td>
<td>“C:\Program Files (x86)\Citrix\System32\WebSocketService.exe”</td>
<td>Local System account</td>
<td>Provides multiple HDX Multimedia services with the initial framework required to perform media redirection between the virtual desktop and the endpoint device.</td>
</tr>
<tr>
<td>Citrix HDX Browser Redirection Service</td>
<td>“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g BrowserRedirSvcs</td>
<td>This account (local CtxSvcHost.exe)</td>
<td>Provides browser content redirection between the endpoint device and the virtual desktop.</td>
</tr>
<tr>
<td>Citrix Port Forwarding Service</td>
<td>“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g PortFwdSvcs</td>
<td>This account (local CtxSvcHost.exe)</td>
<td>Provides port forwarding between the endpoint device and the virtual desktop for browser content redirection.</td>
</tr>
<tr>
<td>Citrix HDX Teams Redirection Service</td>
<td>“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g TeamsSvcs</td>
<td>Local System account</td>
<td>Provides Microsoft Teams redirection between the endpoint device and the virtual desktop.</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

Citrix Workspace app

On the user’s endpoint, the Citrix Workspace app for Windows instantiates a new service called HdxTeams.exe. It does so when Microsoft Teams launches in the VDA and the user tries to call or access peripherals in self-preview. If you don’t see this service, check the following:

1. Ensure that you installed as a minimum the Workspace App version 1905 for Windows. Do you see HdxTeams.exe and the webrpc.dll binaries in the Workspace app installation path?
2. If you validated step 1, do the following to check if HdxTeams.exe is getting launched.
   a) Exit Microsoft Teams on the VDA.
   b) Start services.msc on VDA.
   c) Stop the Citrix HDX Teams Redirection Service.
   d) Disconnect the ICA session.
   e) Connect the ICA session.
   f) Start the Citrix HDX Teams Redirection Service.
   g) Restart the Citrix HDX HTML5 Video Redirection Service.
   h) Launch Microsoft Teams on the VDA.
3. If you still don’t see HdxTeams.exe being launched on the client endpoint, do the following:
   a) Restart the VDA.
   b) Restart the client endpoint.

Support

Citrix and Microsoft jointly support the delivery of Microsoft Teams from Citrix Virtual Apps and Desktops using optimization for Microsoft Teams. This joint support is the result of close collaboration between the two companies. If you have valid support contracts and you experience an issue with this solution, open a support ticket with the vendor whose code you suspect to be causing the issue. That is, Microsoft for Teams or Citrix for the optimization components.

Citrix or Microsoft receives the ticket, triages the issue, and escalates as appropriate. There is no need for you to contact each company’s support team.

When you have a problem, we recommend you click Help > Report a Problem in the Teams UI. VDA-side logs are automatically shared between Citrix and Microsoft to resolve technical issues faster.

Collecting logs

HDXTeams.exe logs can be found on the user’s machine at %TEMP% inside the HDXTeams folder (AppData/Local/Temp/HDXTeams). Look for a .txt file called webrpc_Day_Month_timestamp_Year.txt. When establishing a call, these four ICE phases are required:

• Candidate gathering
• candidate exchange
• Connectivity checks (STUN bind requests)
• Candidate promotion

In the HdxTeams.exe logs, the following entries are the relevant Interactive Connectivity Establishment (ICE) entries. These entries must be there for a call set-up to succeed (see this sample snippet for the gathering stage):

```plaintext
RPCStubs Info: -> device id = \?\display#int3470#4&1835d135&8&uid13424#
{65e8773d-8f56-11d0-a3b9-00a0c9223196 }
{ bf89b5a5-61f7-4127-a279-e187013d7caf }
label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state = HaveLocalOffer
webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering

[...]

>>> begin:sdp
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[...]

>>> begin:sdp
candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
network-cost 10
<<< end:sdp
[...]

>>> begin:sdp
candidate:4271145120 1 udp 1685987671 66.xxx.xxx.xxx 55839 typ srflx
raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1
<<< end:sdp
[...]
```

© 1999-2020 Citrix Systems, Inc. All rights reserved.
If there are multiple ICE candidates, the order of preference is:

1. host  
2. peer reflexive  
3. server reflexive  
4. transport relay

If you encounter an issue and can reproduce it consistently, we recommend clicking Help > Report a problem in Teams. Logs are shared between Citrix and Microsoft to resolve technical issues if you opened a case with Microsoft.

Capturing CDF traces before contacting Citrix Support is also beneficial. For more information, see the Knowledge Center article CDFcontrol.

For recommendations for collecting CDF Traces, see the Knowledge Center article Recommendations for Collecting the CDF Traces.

**VDA side CDF traces - Enable the following CDF trace providers:**
Citrix Virtual Apps and Desktops service

Workspace App side CDF traces - Enable the following CDF trace providers:

Copyed!
Failed!

Windows Media redirection

April 7, 2020

Windows Media redirection controls and optimizes the way servers deliver streaming audio and video to users. By playing the media run-time files on the client device rather than the server, Windows Media redirection reduces the bandwidth requirements for playing multimedia files. Windows Media redirection improves the performance of Windows Media Player and compatible players running on virtual Windows desktops.

If the requirements for Windows Media client-side content fetching are not met, media delivery automatically uses server-side fetching. This method is transparent to users. You can use the Citrix Scout to perform a Citrix Diagnosis Facility (CDF) trace from HostMMTransport.dll to determine the method used. For more information see, Citrix Scout.
Windows Media redirection intercepts the media pipeline at the host server, captures the media data in its native compressed format, and redirects the content to the client device. The client device then recreates the media pipeline to decompress and render the media data received from the host server. Windows Media redirection works well on client devices running a Windows operating system. Those devices have the multimedia framework required to rebuild the media pipeline as it existed on the host server. Linux clients use similar open-source media frameworks to rebuild the media pipeline.

The policy setting **Windows Media Redirection** controls this feature and is **Allowed** by default. Usually, this setting increases audio and video quality rendered from the server to a level that is comparable to content played locally on a client device. In the rare cases, media playing using Windows Media redirection appears worse than media rendered using basic ICA compression and regular audio. You can disable this feature by adding the **Windows Media Redirection** setting to a policy and setting its value to **Prohibited**.

For more information about the policy settings, see [Multimedia policy settings](#).

**Limitation:**

When you’re using Windows Media Player and Remote Audio & Video Extensions (RAVE) enabled inside a session, a black screen might appear. This black screen might appear if you right-click on the video content and select **Always show Now Playing on top**.

Copied!
Failed!

### General content redirection

April 7, 2020

Content redirection allows you to control whether users access information by using applications published on servers or by using applications running locally on user devices.

**Client folder redirection**

Client folder redirection changes the way client-side files are accessible on the host-side session.

- When you enable only client drive mapping on the server, client-side full volumes are automatically mapped to the sessions as Universal Naming Convention (UNC) links.
- When you enable client folder redirection on the server and the user configures it on the Windows desktop device, the portion of the local volume specified by the user is redirected.

**Host to client redirection**

Consider using host to client redirection for specific uncommon use cases. Normally, other forms of content redirection might be better. We support this type of redirection only on Multi-session OS VDAs
Citrix Virtual Apps and Desktops service

and not on Single-session OS VDAs.

Local App Access and URL redirection

Local App Access seamlessly integrates locally installed Windows applications into a hosted desktop environment. It does so without changing from one computer to another.

HDX technology provides generic USB redirection for specialty devices that don’t have any optimized support or where it is unsuitable.

Client folder redirection

August 21, 2020

Client folder redirection changes the way client-side files are accessible on the host-side session. If you enable only client drive mapping on the server, client-side full volumes are automatically mapped as Universal Naming Convention (UNC) links to the sessions. When you enable client folder redirection on the server and the user configures it on the user device, the portion of the local volume specified by the user is redirected.

Only the user-specified folders appear as UNC links inside sessions. That is, instead of the complete file system on the user device. If you disable UNC links through the registry, client folders appear as mapped drives inside the session.

Client folder redirection is supported on Windows Single-session OS machines only.

Client folder redirection for an external USB drive is not saved on detaching and reattaching the device.

Enable client folder direction on the server. Then, on the client device, specify which folders to redirect. The application you use to specify the client folder options is included with the Citrix Workspace app supplied with this release.

Requirements:

For servers:

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

For clients:

- Windows 10, 32-bit and 64-bit editions (minimum version 1607)
- Windows 8.1, 32-bit and 64-bit editions (including Embedded edition)
Citrix Virtual Apps and Desktops service

- Windows 7, 32-bit and 64-bit editions (including Embedded edition)

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.

1. On the server:
   a) Create a key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
   b) Create a REG_DWORD value.
      - Name: CFROnlyModeAvailable
      - Type: REG_DWORD
      - Data: Set to 1

2. On the user device:
   a) Ensure that the latest version of Citrix Workspace app is installed.
   b) From the Citrix Workspace app installation directory, start CtxCFRUI.exe.
   c) Choose the Custom radio button and add, edit, or remove folders.
   d) Disconnect and reconnect your sessions for the setting to take effect.

Host to client redirection

May 15, 2020

Content redirection allows you to control how users access information. You can control whether users access information by using applications published on servers or applications running locally on user devices.

Host to client redirection is one type of content redirection. It is supported only on Multi-session OS VDAs (not Single-session OS VDAs).

- When host to client redirection is enabled, URLs are intercepted at the server VDA and sent to the user device. The web browser or multimedia player on the user device opens these URLs.
- If you enable host to client redirection and the user device fails to connect to a URL, the URL is redirected back to the server VDA.
- When host to client redirection is disabled, users open the URLs using web browsers or multimedia players on the server VDA.
• When host to client redirection is enabled, users cannot disable it.

Host to client redirection was previously known as **server to client redirection**.

**When to use host to client redirection**

You might consider using host to client redirection in specific but uncommon cases, for performance, compatibility, or compliance. Normally, other forms of content redirection are better.

**Performance:**

You can use host to client redirection for performance. Whenever an application is installed on the user device, it is used in preference to an application on the VDA.

Host to client redirection improves performance only under specific conditions, because the VDA already optimizes Adobe Flash and other types of multimedia content. First, consider using the other approaches (policy settings) noted in the tables in this article, rather than host to client redirection. Those settings offer more flexibility and usually give a better user experience, particularly for less-powerful user devices.

**Compatibility:**

You can use host to client redirection for compatibility in the following use cases:

- You use content types other than HTML or multimedia (for example, a custom URL type).
- You use a legacy media format (such as Real Media) that the VDA multimedia player using multimedia redirection doesn’t support.
- The application for the content type is used by only a few users who already have the application installed on their user device.
- The VDA cannot access certain websites (for example, websites internal to another organization).

**Compliance:**

You can use host to client redirection for compliance in the following use cases:

- The application or content licensing agreement does not permit publishing via the VDA.
- Organizational policy does not permit a document being uploaded to the VDA.

Some situations are more likely in complex environments, and also if the user device and the VDA belong to different organizations.

**User device considerations**

Environments can have many different types of user devices.
## Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>User device</th>
<th>Situation or environment</th>
<th>Content redirection approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tablet</td>
<td>-</td>
<td>Any approach (see next table)</td>
</tr>
<tr>
<td>Laptop PC</td>
<td>-</td>
<td>Any approach (see next table)</td>
</tr>
<tr>
<td>Desktop PC</td>
<td>Users use a wide range of apps installed on the user device</td>
<td>Any approach (see next table)</td>
</tr>
<tr>
<td>Desktop PC</td>
<td>Users use only a few known apps that are installed on the user device</td>
<td>Local App Access</td>
</tr>
<tr>
<td>Desktop PC</td>
<td>Users use no apps installed on the user device</td>
<td>Multimedia redirection</td>
</tr>
<tr>
<td>Thin client</td>
<td>Vendor supports multimedia redirection and host to client redirection</td>
<td>Any approach (see next table)</td>
</tr>
<tr>
<td>Zero client</td>
<td>Vendor supports multimedia redirection</td>
<td>Multimedia redirection</td>
</tr>
</tbody>
</table>

### Use the following examples to help guide your content redirection approach.

<table>
<thead>
<tr>
<th>URLs link</th>
<th>Situation or environment</th>
<th>Content redirection approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>A webpage or document</td>
<td>The VDA cannot access the URL.</td>
<td>Host to client redirection</td>
</tr>
<tr>
<td>A multimedia file or stream</td>
<td>The VDA has a compatible multimedia player.</td>
<td>Multimedia redirection</td>
</tr>
<tr>
<td>A multimedia file or stream</td>
<td>The VDA does not have a compatible multimedia player.</td>
<td>Host to client redirection</td>
</tr>
<tr>
<td>A document</td>
<td>The VDA does not have an application for that document type.</td>
<td>Host to client redirection</td>
</tr>
<tr>
<td>A document</td>
<td>Do not download the document to the user device.</td>
<td>No redirection</td>
</tr>
<tr>
<td>A document</td>
<td>Do not upload the document to the VDA.</td>
<td>Host to client redirection</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>URL link</th>
<th>Situation or environment</th>
<th>Content redirection approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>A custom URL type</td>
<td>The VDA does not have an application for that custom URL type.</td>
<td>Host to client redirection</td>
</tr>
</tbody>
</table>

These Citrix Workspace apps support Host to client redirection:

- Citrix Workspace app for Windows
- Citrix Workspace app for Mac
- Citrix Workspace app for Linux
- Citrix Workspace app for HTML5
- Citrix Workspace app for Chrome

To use host to client redirection, the user device must have a web browser, multimedia player, or other application that is suitable for the content. If the user device is one of the following, confirm it has suitable applications and power.

- Thin client
- Zero client

User devices enabled for Local App Access use a different mechanism for content redirection, and do not require host to client content redirection.

You can use Citrix policies to prevent host to client content redirection for unsuitable devices.

**How users experience host to client redirection**

Host to client redirection is used when URLs are:

- Embedded as hyperlinks in an application (for example, in an email message or document).
- Selected through VDA application menus or dialogs, if the application uses the Windows ShellExecuteEx API.
- Typed in the Windows Run dialog.

Host to client redirection is not used for URLs in a web browse. That is, either in a webpage or typed in the address bar of the web browser.

**Note**

If users change their default web browser on the VDA, that change can interfere with host to client redirection for applications. An example of changing the default web browser is using Set Default Programs.
When host to client content redirection is enabled, the app that opens the URL uses the user device configuration for the URL type and the content type. For example:

- An HTTP URL that has an HTML content type opens in the default web browser.
- An HTTP URL that has a PDF content type might open in the default web browser, or it might open in another application.

Host to client content redirection doesn’t control this user device configuration. If you do not control the configuration of the user device, consider using multimedia redirection, rather than host to client content redirection.

The following URL types are opened locally through user devices when host to client redirection is enabled:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

To delete and add URL types, you can change the list of URL types for host to client redirection. URL types include custom types.

### Enable host to client redirection

Enabling host to client redirection starts by enabling a Citrix policy setting.

The Host to client redirection policy setting is located in the File Redirection policy settings section. By default, this setting is disabled.

In addition, you might need to set registry keys and Group Policy for the server VDAs, depending on the VDA OS.

- If the server VDA is Windows Server 2008 R2 SP1, you do not need to set registry keys or Group Policy.
- If the server VDA is Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016, you must set registry keys and Group Policy.

**Warning**

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

1. Copy the text between “Reg file start” and “Reg file end” in the example, and paste it in Notepad.
2. Save the Notepad file using “Save As” and the type All Files and the name ServerFTA.reg.
3. Distribute the ServerFTA.reg file to the servers using Active Directory Group Policy.

```
1 -- Reg file start --
2
3     Windows Registry Editor Version 5.00
4
5     [HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]
6
7     @="\"C:\Program Files (x86)\Citrix\HDX\bin\iexplore.exe\" %1"
8
9     [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]
10
11    @="ServerFTA"
12
13    [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]
14
15    "ApplicationDescription"="Server FTA URL."
16
17    "ApplicationIcon"="C:\Program Files (x86)\Citrix\HDX\bin\iexplore.exe,0"
18
19    "ApplicationName"="ServerFTA"
20
21    [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\URLAssociations]
22
23    "http"="ServerFTAHTML"
24
25    "https"="ServerFTAHTML"
26
27    [HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]
28
29    "Citrix.ServerFTA"="SOFTWARE\Citrix\ServerFTA\Capabilities"
30
31 -- Reg file end --
```

Group Policy changes

Create an XML file. Copy the text between “xml file start” and “xml file end” the example, paste it in the XML file, and then save the file as ServerFTAdefaultPolicy.xml.

```
1 -- xml file start --
2
```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>
  <Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />
  <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />
</DefaultAssociations>

From the current Group Policy management console, navigate to: Computer configuration > Administrative Templates > Windows Components > File Explorer > Set a default associations configuration file, and provide the ServerFTAdefaultPolicy.xml file you created.

**Change the list of URL types for host to client redirection**

To change the list of URL types for host to client redirection, set the following registry key on the server VDA.

Key: HKLM\Software\Wow6432Node\Citrix\SFTA

To delete URL types from the list, set DisableServerFTA and NoRedirectClasses:

Name: DisableServerFTA
Type: REG_DWORD
Data: 1

Name: NoRedirectClasses
Type: REG_MULTI_SZ
Data: Specify any combination of the values: http, https, rtsp, rtspu, pnm, or mms. Type multiple values on separate lines. For example:

http
https
rtsp

To add URL types to the list, set ExtraURLProtocols:

Name: ExtraURLProtocols
Type: REG_MULTI_SZ

Data: Specify any combination of URL types. Each URL type must include the :// suffix; separate multiple values by using semicolons. For example:
customtype1://;customtype2://

Enable host to client redirection for a specific set of websites

To enable host to client redirection for a specific set of websites, set the following registry key on the server VDA.

Key: HKLM\Software\Wow6432Node\Citrix\SFTA

Name: ValidSites

Type: REG_MULTI_SZ

Data: Specify any combination of fully qualified domain names (FQDNs). Type multiple FQDNs on separate lines. An FQDN can include a wildcard in the leftmost position only. This wildcard matches a single level of domain, which is consistent with the rules in RFC 6125. For example:

www.example.com
\*.example.com

Local App Access and URL redirection

August 21, 2020

Introduction

Local App Access seamlessly integrates locally installed Windows applications into a hosted desktop environment without switching from one desktop to another. With Local App Access, you can:

- Access applications installed locally on a physical laptop, PC, or other device directly from the virtual desktop.
- Provide a flexible application delivery solution. If users have local applications that you cannot virtualize or that IT does not maintain, those applications still behave as though they are installed on a virtual desktop.
Citrix Virtual Apps and Desktops service

- Eliminate the double-hop latency when applications are hosted separately from the virtual desktop. Do so by putting a shortcut to the published application on the user’s Windows device.
- Use applications such as:
  - Video conferencing software such as GoToMeeting.
  - Specialty or niche applications that are not yet virtualized.
  - Applications and peripherals that would otherwise transfer large amounts of data from a user device to a server and back to the user device. For example, DVD burners and TV tuners.

In Citrix Virtual Apps and Desktops, hosted desktop sessions use URL redirection to start Local App Access applications. URL redirection makes the application available under more than one URL address. It launches a local browser (based on the browser’s URL blacklist) by selecting embedded links within a browser in a desktop session. If you navigate to a URL that is not present in the blacklist, the URL is opened in the desktop session again.

URL redirection works only for desktop sessions, not application sessions. The only redirection feature you can use for application sessions is host-to-client content redirection, which is a type of server FTA (File Type Association) redirection. This FTA redirects certain protocols to the client, such as HTTP, HTTPS, RTSP, or MMS. For example, if you only open embedded links with HTTP, the links directly open with the client application. There is no URL blacklist or whitelist support.

When Local App Access is enabled, URLs that are displayed to users as links from locally running applications, from user-hosted applications, or as shortcuts on the desktop are redirected in one of the following ways:

- From the user’s computer to the hosted desktop
- From the Citrix Virtual Apps and Desktops server to the user’s computer
- Rendered in the environment in which they are started (not redirected)

To specify the redirection path of content from specific websites, configure the URL whitelist and URL blacklist on the Virtual Delivery Agent. Those lists contain multi-string registry keys that specify the URL redirection policy settings. For more information, see the Local App Access policy settings.

URLs can be rendered on the VDA with the following exceptions:

- Geo/Locale information — Websites that require locale information, such as msn.com or news.google.com (opens a country specific page based on the Geo). For example, if the VDA is provisioned from a data center in the UK and the client is connecting from India, the user expects to see in.msn.com. Instead, the user sees uk.msn.com.
- Multimedia content — Websites containing rich media content, when rendered on the client device, give the end users a native experience and also save bandwidth even in high latency networks. This feature redirects sites with other media types such as Silverlight. This process is in a secure environment. That is, the URLs that the administrator approves are run on the client...
while the rest of the URLs are redirected to the VDA.

In addition to URL redirection, you can use FTA redirection. FTA starts local applications when a file is encountered in the session. If the local app is started, the local app must have access to the file to open it. Therefore, you can only open files that reside on network shares or on client drives (using client drive mapping) using local applications. For example, when opening a PDF file, if a PDF reader is a local app, then the file opens using that PDF reader. Because the local app can access the file directly, there is no network transfer of the file through ICA to open the file.

Requirements, considerations, and limitations

We support Local App Access on the valid operating systems for VDAs for Windows Multi-session OS and for VDAs for Windows Single-session OS. Local App Access requires Citrix Workspace app for Windows version 4.1 (minimum). The following browsers are supported:

- Internet Explorer 11. You can use Internet Explorer 8, 9, or 10, but Microsoft supports (and Citrix recommends using) version 11.
- Firefox 3.5 through 21.0
- Chrome 10

Review the following considerations and limitations when using Local App Access and URL redirection.

- Local App Access is designed for full-screen, virtual desktops spanning all monitors:
  - The user experience can be confusing if you use Local App Access with a virtual desktop that runs in windowed mode or does not cover all monitors.
  - Multiple monitors — When one monitor is maximized, it becomes the default desktop for all applications started in that session. This default occurs even if the subsequent applications typically start on another monitor.
  - The feature supports one VDA. There is no integration with multiple concurrent VDAs.
- Some applications can behave unexpectedly, affecting users:
  - The drive letters might confuse users, such as local C: rather than virtual desktop C: drive.
  - Available printers in the virtual desktop are not available to local applications.
  - Applications that require elevated permissions cannot be started as client-hosted applications.
  - There is no special handling for single-instance applications (such as Windows Media Player).
  - Local applications appear with the Windows theme of the local machine.
  - Full-screen applications are not supported. These applications include applications that open to a full screen, such as PowerPoint slide shows or photo viewers that cover the entire desktop.
  - Local App Access copies the properties of the local application (such as the shortcuts on the client’s desktop and Start menu) on the VDA. However, it does not copy other proper-
Application and Desktops service

ties such as shortcut keys and read-only attributes.

– Applications that customize how overlapping window order is handled can have unpredictable results. For example, some windows might be hidden.

– Shortcuts are not supported, including My Computer, Recycle Bin, Control Panel, Network Drive shortcuts, and folder shortcuts.

– The following file types and files are not supported: custom file types, files with no associated programs, zip files, and hidden files.

– Taskbar grouping is not supported for mixed 32-bit and 64-bit client-hosted or VDA applications. That is, grouping 32-bit local applications with 64-bit VDA applications.

– Applications cannot be started using COM. For example, if you click an embedded Office document from within an Office application, the process start cannot be detected, and the local application integration fails.

• Double-hop scenarios, where a user is starting a virtual desktop from within another virtual desktop session, are not supported.

• URL redirection supports only explicit URLs (that is, URLs appearing in the browser’s address bar or found using the in-browser navigation, depending on the browser).

• URL redirection works only with desktop sessions, not with application sessions.

• The local desktop folder in a VDA session does not allow users to create files.

• Multiple instances of a locally running application behave according to the taskbar settings established for the virtual desktop. However, shortcuts to locally running applications are not grouped with running instances of those applications. They are also not grouped with running instances of hosted applications or pinned shortcuts to hosted applications. Users can close only windows of locally running applications from the Taskbar. Although users can pin local application windows to the desktop Taskbar and Start menu, the applications might not start consistently when using these shortcuts.

Interaction with Windows

The Local App Access interaction with Windows includes the following behaviors.

• Windows 8 and Windows Server 2012 shortcut behavior
  – Windows Store applications installed on the client are not enumerated as part of Local App Access shortcuts.
  – Image and video files are opened by default using Windows store applications. However, Local App Access enumerates the Windows store applications and opens shortcuts with desktop applications.

• Local Programs
  – For Windows 7, the folder is available in the Start menu.
  – For Windows 8, Local Programs is available only when the user chooses All Apps as a category from the Start screen. Not all subfolders are displayed in Local Programs.
Citrix Virtual Apps and Desktops service

- Windows 8 graphics features for applications
  - Desktop applications are restricted to the desktop area and are covered by the Start screen and Windows 8 style applications.
  - Local App Access applications do not behave like desktop applications in multi-monitor mode. In multi-monitor mode, the Start screen and the desktop display on different monitors.
- Windows 8 and Local App Access URL Redirection
  - Because Windows 8 Internet Explorer has no add-ons enabled, use desktop Internet Explorer to enable URL redirection.
  - In Windows Server 2012, Internet Explorer disables add-ons by default. To implement URL Redirection, disable the Internet Explorer enhanced configuration. Then reset the Internet Explorer options and restart to ensure that add-ons are enabled for standard users.

Configure Local App Access and URL redirection

To use Local App Access and URL redirection with Citrix Workspace app:

- Install Citrix Workspace app on the local client machine. You can enable both features during the Citrix Workspace app installation or you can enable Local App Access template using the Group Policy editor.
- Set the Allow local app access policy setting to Enabled. You can also configure URL whitelist and blacklist policy settings for URL redirection. For more information, see Local App Access policy settings.

Enable Local App Access and URL redirection

To enable Local App Access for all local applications, follow these steps:

1. Start Citrix Studio.
   - For on-premises deployments, open Citrix Studio from the Start menu.
   - For Cloud service deployments, go to Citrix Cloud > Virtual Apps and Desktops service > Manage tab.
2. In the Studio navigation pane, click Policies.
3. In the Actions pane, click Create Policy.
4. In the Create Policy window, type “Allow Local App Access” in the search box and then click Select.
5. In the Edit Setting window, select Allowed. By default, the Allow local app access policy is prohibited. When this setting is allowed, the VDA allows the end-user to decide whether published applications and Local App Access shortcuts are enabled in the session. (When this setting is prohibited, both published applications and Local App Access shortcuts do not work for the VDA.) This policy setting applies to the entire machine and the URL redirection policy.
6. In the Create Policy window, type “URL redirection white list” in the search box and then click **Select**. The URL redirection white list specifies URLs to open in the default browser of the remote session.

7. In the Edit Setting window, click **Add** to add the URLs and then click **OK**.

8. In the Create Policy window, type “URL redirection black list” in the search box and then click **Select**. The URL redirection black list specifies URLs that are redirected to the default browser running on the endpoint.

9. In the Edit Setting window, click **Add** to add the URLs and then click **OK**.

10. On the Settings page, click **Next**.

11. On the Users and Machines page, assign the policy to the applicable Delivery Groups and then click **Next**.

12. On the Summary page, review the settings and then click **Finish**.

To enable URL redirection for all local applications during Citrix Workspace app installation, follow the steps below:

1. Enable URL redirection when you install Citrix Workspace app for all users on a machine. Doing so also registers the browser add-ons required for URL redirection.

2. From the command prompt, run the appropriate command to install the Citrix Workspace app using one of the following options:
   - For CitrixReceiver.exe, use `ALLOW_CLIENTHOSTEDAPPSURL=1`.
   - For CitrixReceiverWeb.exe, use `ALLOW_CLIENTHOSTEDAPPSURL=1`.

---

**Enable the Local App Access template using the Group Policy editor**

**Note:**
- Before you enable the Local App Access template using the Group Policy editor, add the receiver.admx/adml template files to the local GPO. For more information, see Configuring the Group Policy Object administrative template.
- Citrix Workspace app for Windows template files are available in the local GPO in Administrative Templates > Citrix Components > Citrix Workspace folder only when you add the CitrixBase.admx/CitrixBase.adml to the %systemroot%\policyDefinitions folder.

To enable the Local App Access template using the Group Policy editor, follow these steps:

1. Run `gpedit.msc`.

2. Go to **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Workspace > User Experience**.

3. Click **Local App Access settings**.

4. Select **Enabled** and then select **Allow URL Redirection**. For URL redirection, register browser add-ons using the command line described in the Register browser add-ons section further down in this article.
Provide access only to published applications

You can provide access to published applications using one of the following two ways:

Use the Registry Editor.

1. On the server where Citrix Studio is installed, run regedit.exe.
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio.
3. Add the REG_DWORD entry ClientHostedAppsEnabled and a value of 1. (A 0 value disables Local App Access.)

Use the PowerShell SDK.

1. Open PowerShell on the machine where the Delivery Controller is running.
2. Enter the following command: set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true".

To have access to Add Local App Access Application in a Cloud service deployment, use the Citrix Virtual Apps and Desktops Remote PowerShell SDK. For more information, see Citrix Virtual Apps and Desktops Remote PowerShell SDK.

1. Download the installer:
   https://download.apps.cloud.com/CitrixPoshSdk.exe
2. Run these commands:
   a) asnp citrix.*
   b) Get-XdAuthentication
3. Enter the following command: set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true".

After you complete the applicable preceding steps, follow these steps to continue.

1. Open Citrix Studio from the Start menu.
2. In the Studio navigation pane, click Applications.
3. In the upper middle pane, right-click the blank area and select Add Local App Access Application from the context menu. You can also click Add Local App Access Application in the Actions pane. To display the Add Local App Access Application option in the Actions pane, click Refresh.
4. Publish Local App Access application.
   - The Local Application Access wizard launches with an Introduction page, which you can remove from future launches of the wizard.
   - The wizard guides you through the Groups, Location, Identification, Delivery, and Summary pages described below. When you are finished with each page, click Next until you reach the Summary page.
Citrix Virtual Apps and Desktops service

- On the Groups page, select one or more Delivery Groups where the new applications will be added, and then click **Next**.

- On the Location page, type the full executable path of the application on the user’s local machine, and type the path to the folder where the application is located. Citrix recommends that you use the system environment variable path; for example, `%ProgramFiles(x86)\InternetExplorer\iexplore.exe`.

- On the Identification page, accept the default values or type the information that you want and then click **Next**.

- On the Delivery page, configure how this application is delivered to users and then click **Next**. You can specify the icon for the selected application. You can also specify whether the shortcut to the local application on the virtual desktop will be visible on the Start menu, the desktop, or both.

- On the Summary page, review the settings and then click **Finish** to exit the Local Application Access wizard.

**Register browser add-ons**

**Note:** The browser add-ons required for URL redirection are registered automatically when you install Citrix Workspace app from the command line using the /ALLOW_CLIENTHOSTEDAPPSURL=1 option.

You can use the following commands to register and unregister one or all add-ons:

- To register add-ons on a client device: `<client-installation-folder>\redirector.exe /reg<browser>`
- To unregister add-ons on a client device: `<client-installation-folder>\redirector.exe /unreg<browser>`
- To register add-ons on a VDA: `<VDAinstallation-folder>\VDARedirector.exe /reg<browser>`
- To unregister add-ons on a VDA: `<VDAinstallation-folder>\VDARedirector.exe /unreg<browser>`

Where `<browser>` is Internet Explorer, Firefox, Chrome, or All.

For example, the following command registers Internet Explorer add-ons on a device running Citrix Workspace app.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

The following command registers all add-ons on a Windows Multi-session OS VDA.

C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regAll

© 1999-2020 Citrix Systems, Inc. All rights reserved. 395
**URL interception across browsers**

- By default, Internet Explorer redirects the specified URL. If the URL is not in the blacklist but the browser or website redirects it to another URL, the final URL is not redirected. It is not redirected even if it is on the blacklist.

For URL redirection to work correctly, enable the add-on when prompted by the browser. If the add-ons that are using Internet options or the add-ons in the prompt are disabled, URL redirection does not work correctly.

- The Firefox add-ons always redirect the URLs.

When an add-on is installed, Firefox prompts to allow or prevent installing the add-on on a new tab page. Allow the add-on for the feature to work.

- The Chrome add-on always redirects the final URL that is navigated, and not the entered URLs.

The extensions have been installed externally. When you disable the extension, the URL redirection feature does not work in Chrome. If the URL redirection is required in Incognito mode, allow the extension to run in that mode in the browser settings.

**Configure local application behavior on logoff and disconnect**

**Note:**
If you do not follow these steps to configure the settings, by default, local applications continue to run when a user logs off or disconnects from the virtual desktop. After reconnection, local applications are reintegrated if they are available on the virtual desktop.

1. On the hosted desktop, run `regedit.msc`.

2. **Navigate to** \HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies \Session State.

   For a 64-bit system, navigate to \HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\ Client Hosted Apps\Policies\Session State.

3. **Add the REG_DWORD entry** `Terminate` and one of the values:

   - 1 - Local applications continue to run when a user logs off or disconnects from the virtual desktop. Upon reconnection, local applications are reintegrated if they are available in the virtual desktop.
   - 3 - Local applications close when a user logs off or disconnects from the virtual desktop.
Citrix Virtual Apps and Desktops service

Generic USB redirection and client drive considerations

August 21, 2020

HDX technology provides optimized support for most popular USB devices. Optimized support offers an improved user experience with better performance and bandwidth efficiency over a WAN. Optimized support is usually the best option, especially in high latency or security-sensitive environments.

HDX technology provides generic USB redirection for specialty devices that don’t have optimized support or where it is unsuitable, for example:

- The USB device has more advanced features that are not part of optimized support, such as a mouse or webcam having more buttons.
- Users need functions which are not part of optimized support.
- The USB device is a specialized device, such as test and measurement equipment or an industrial controller.
- An application requires direct access to the device as a USB device.
- The USB device only has a Windows driver available. For example, a smart card reader might not have a driver available for Citrix Workspace app for Android.
- The version of Citrix Workspace app does not provide any optimized support for this type of USB device.

With generic USB redirection:

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

Important:

- Generic USB redirection can be used together with optimized support. If you enable generic USB redirection, configure Citrix USB devices policy settings for both generic USB redirection and optimized support.
- The Citrix policy setting in Client USB device optimization rules is a specific setting for generic USB redirection, for a particular USB device. It doesn’t apply to optimized support as described here.
- When brokering a session using Citrix software to an Azure Virtual Machine, Citrix provides best effort support for USB redirection to the Azure Virtual Machine. We support fixing a Citrix software problem, but we do not support the underlying Azure Virtual Machine.

Performance considerations for USB devices

Network latency and bandwidth can affect user experience and USB device operation when using generic USB redirection for some types of USB devices. For example, timing-sensitive devices might
Citrix Virtual Apps and Desktops service

not operate correctly over high-latency low-bandwidth links. Use optimized support instead where possible.

Some USB devices require high bandwidth to be usable, for example a 3D mouse (used with 3D apps that also typically require high bandwidth). If bandwidth cannot be increased, you might be able to mitigate the issue by tuning bandwidth usage of other components using the bandwidth policy settings. For more information, see Bandwidth policy settings for Client USB device redirection, and Multi-stream connection policy settings.

Security considerations for USB devices

Some USB devices are security-sensitive by nature, for example, smart card readers, fingerprint readers, and signature pads. Other USB devices such as USB storage devices can be used to transmit data that might be sensitive.

USB devices are often used to distribute malware. Configuration of Citrix Workspace app and Citrix Virtual Apps and Desktops can reduce, but not eliminate, risk from these USB devices. This situation applies whether generic USB redirection or optimized support is used.

Important:

For security-sensitive devices and data, always secure the HDX connection using either TLS or IPsec.

Only enable support for the USB devices that you need. Configure both generic USB redirection and optimized support to meet this need.

Provide guidance to users for safe use of USB devices:

- Use only USB devices that have been obtained from a trustworthy source.
- Don’t leave USB devices unattended in open environments - for example, a flash drive in an internet cafe.
- Explain the risks of using a USB device on more than one computer.

Compatibility with generic USB redirection

Generic USB redirection is supported for USB 2.0 and earlier devices. Generic USB redirection is also supported for USB 3.0 devices connected to a USB 2.0 or USB 3.0 port. Generic USB redirection does not support USB features introduced in USB 3.0, such as super speed.

These Citrix Workspace apps support generic USB redirection:

- Citrix Workspace app for Windows, see Configuring application delivery.
- Citrix Workspace app for Mac, see Citrix Workspace app for Mac.
- Citrix Workspace app for Linux, see Optimize.
Citrix Virtual Apps and Desktops service

- Citrix Workspace app for Chrome OS, see Citrix Workspace app for Chrome.

For Citrix Workspace app versions, see the Citrix Workspace app feature matrix.

If you are using earlier versions of Citrix Workspace app, see the Citrix Workspace app documentation to confirm that generic USB redirection is supported. See Citrix Workspace app documentation for any restrictions on USB device types that are supported.

Generic USB redirection is supported for desktop sessions from VDA for Single-session OS version 7.6 through current.

Generic USB redirection is supported for desktop sessions from VDA for Multi-session OS version 7.6 through current, with these restrictions:

- The VDA must be running Windows Server 2012 R2 or Windows Server 2016.
- The USB device drivers must be fully compatible with Remote Desktop Session Host (RDSH) for the VDA OS (Windows 2012 R2), including full virtualization support.

Some types of USB devices are not supported for generic USB redirection because it would not be useful to redirect them:

- USB modems.
- USB network adapters.
- USB hubs. The USB devices connected to USB hubs are handled individually.
- USB virtual COM ports. Use COM port redirection rather than generic USB Redirection.

For information on USB devices that have been tested with generic USB redirection, see Citrix Ready Marketplace. Some USB devices do not operate correctly with generic USB redirection.

Configure generic USB redirection

You can control, and separately configure, which types of USB devices use generic USB redirection:

- On the VDA, using Citrix policy settings. For more information, see Redirection of client drives and user devices and USB devices policy settings in the Policy settings reference.
- In Citrix Workspace app, using Citrix Workspace app-dependent mechanisms. For example, an Administrative Template controls registry settings that configure Citrix Workspace app for Windows. By default, USB redirection is allowed for certain classes of USB devices and denied for others. For more information, see Configure in the Citrix Workspace app for Windows documentation.

This separate configuration provides flexibility. For example:

- If two different organizations or departments are responsible for Citrix Workspace app and VDA, they can enforce control separately. This configuration applies when a user in one organization accesses an application in another organization.
Citrix policy settings can control USB devices that are allowed only for certain users or for users connecting only over a LAN (rather than by using Citrix Gateway).

Enable generic USB redirection

To enable generic USB Redirection, and not require manual redirection by the user, configure both Citrix policy settings and Citrix Workspace app connections preferences.

In Citrix policy settings:

1. Add the **Client USB device redirection** to a policy and set its value to **Allowed**.

```
[Image: Edit Setting]
```

2. (Optional) To update the list of USB devices available for redirection, add the **Client USB device redirection rules** setting to a policy and specify the USB policy rules.

In Citrix Workspace app:

3. Specify that devices are connected automatically without manual redirection. You can do this using an Administrative template or in Citrix Workspace app for Windows > Preferences > Connections.
If you specified USB policy rules for the VDA in the previous step, specify those same policy rules for Citrix Workspace app.

For thin clients, consult the manufacturer for details of USB support and any required configuration.

**Configuring the types of USB devices available for generic USB redirection**

USB devices are automatically redirected when USB support is enabled and the USB user preference settings are set to connect USB devices automatically. USB devices are also automatically redirected when the connection bar is not present.

Users can explicitly redirect devices that are not automatically redirected by selecting the devices from the USB device list. For more information, the Citrix Workspace app for Windows user help article, *Display your devices in the Desktop Viewer*. 
To use generic USB redirection rather than optimized support, you can either:

- In Citrix Workspace app, manually select the USB device to use generic USB redirection, choose **Switch to generic** from the Devices tab of the Preferences dialog box.
- Automatically select the USB device to use generic USB redirection, by configuring auto-redirection for the USB device type (for example, AutoRedirectStorage=1) and set USB user preference settings to automatically connect USB devices. For more information, see [Configure automatic redirection of USB devices](#).

**Note:**

Only configure generic USB redirection for use with a webcam if the webcam is found to be incompatible with HDX multimedia redirection.

To prevent USB devices from ever being listed or redirected, you can specify device rules for Citrix Workspace app and the VDA.

For generic USB redirection, you need to know at least the USB device class and subclass. Not all USB devices use their obvious USB device class and subclass. For example:
Citrix Virtual Apps and Desktops service

- Pens use the mouse device class.
- Smart card readers can use the vendor-defined or HID device class.

For more precise control, you need to know the Vendor ID, Product ID, and Release ID. You can get this information from the device vendor.

**Important:**

Malicious USB devices might present USB device characteristics that do not match their intended usage. Device rules are not intended to prevent this behavior.

You control the USB devices available for generic USB redirection by specifying USB device redirection rules for both VDA and Citrix Workspace app, to override the default USB policy rules.

**For the VDA:**

- Edit the administrator override rules for the Multi-session OS machines through group policy rules. The Group Policy Management Console is included on the installation media:
  - For x64: dvd root \os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi
  - For x86: dvd root \os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi

**At Citrix Workspace app for Windows:**

- Edit the user device registry. An Administrative template (ADM file) is included on the installation media so you can change the user device through Active Directory Group Policy:
  
dvd root \os\lang\Support\Configuration\icaclient_usb.adm

**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.

The product default rules are stored in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. Do not edit these product default rules. Instead, use them as a guide for creating administrator override rules, which is explained later in this article. The GPO overrides are evaluated before the product default rules.

The administrator override rules are stored in HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. GPO policy rules take the format `{Allow: | Deny:} {tag=value}` expressions separated by white space.

The following tags are supported:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VID</td>
<td>Vendor ID from the device descriptor</td>
</tr>
</tbody>
</table>
Tag | Description
---|---
PID | Product ID from the device descriptor
REL | Release ID from the device descriptor
Class | Class from either the device descriptor or an interface descriptor; see the USB website at [http://www.usb.org/](http://www.usb.org/) for available USB Class Codes
SubClass | Subclass from either the device descriptor or an interface descriptor
Prot | Protocol from either the device descriptor or an interface descriptor

When creating policy rules, note the following:

- Rules are case-insensitive.
- Rules can have an optional comment at the end, introduced by `##`. A delimiter is not required, and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- White space is used as a separator, but cannot appear in the middle of a number or identifier. For example, Deny: Class = 08 SubClass=05 is a valid rule, but Deny: Class=0 Sub Class=05 is not.
- Tags must use the matching operator `=`. For example, VID=1230.
- Each rule must start on a new line or form part of a semicolon-separated list.

**Note:**

If you are using the ADM template file, you must create rules on a single line, as a semicolon-separated list.

**Examples:**

- The following example shows an administrator-defined USB policy rule for vendor and product identifiers:

  Allow: VID=046D PID=C626 ## Allow Logitech SpaceNavigator 3D Mouse
  Deny: VID=046D ## Deny all Logitech products

- The following example shows an administrator-defined USB policy rule for a defined class, subclass, and protocol:

  Deny: Class=EF SubClass=01 Prot=01 ## Deny MS Active Sync devices
  Allow: Class=EF SubClass=01 ## Allow Sync devices
  Allow: Class=EF ## Allow
Use and remove USB devices

Users can connect a USB device before or after starting a virtual session. When using Citrix Workspace app for Windows, the following apply:

- Devices connected after a session begins appear immediately in the USB menu of the Desktop Viewer.
- If a USB device is not redirecting properly, you can try to resolve the problem by waiting to connect the device until after the virtual session starts.
- To avoid data loss, use the Windows “Safely Remove Hardware” icon before removing the USB device.

Security controls for USB mass storage devices

Optimized support is provided for USB mass storage devices. This support is part of Citrix Virtual Apps and Desktops client drive mapping. Drives on the user device are automatically mapped to drive letters on the virtual desktop when users log on. The drives are displayed as shared folders that have mapped drive letters. To configure client drive mapping, use the Client removable drives setting. This setting is in the File Redirection policy settings section of the ICA policy settings.

With USB mass storage devices you can use either Client drive mapping or generic USB redirection, or both. Control them using Citrix policies. The main differences are:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Client drive mapping</th>
<th>Generic USB redirection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled by default</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Read-only access configurable</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Encrypted device access</td>
<td>Yes, if encryption is unlocked before the device is accessed</td>
<td>Yes</td>
</tr>
<tr>
<td>BitLocker To Go devices</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Safe to delete device during a</td>
<td>No</td>
<td>Yes, provided users follow operating system</td>
</tr>
<tr>
<td>session</td>
<td></td>
<td>recommendations for safe removal</td>
</tr>
</tbody>
</table>

If both generic USB redirection and the client drive mapping policies are enabled and a mass storage
device is inserted either before or after a session starts, it is redirected using client drive mapping. When both generic USB redirection and the client drive mapping policies are enabled and a device is configured for automatic redirection and a mass storage device is inserted either before or after a session starts, it is redirected using generic USB redirection. For more information, see Knowledge Center article CTX123015.

**Note:**
USB redirection is supported over lower bandwidth connections, for example 50 Kbps. However, copying large files doesn’t work.

**Control file access with client drive mapping**

You can control whether users can copy files from their virtual environments to their user devices. By default, files and folders on mapped client-drives are available in read/write mode from within the session.

To prevent users from adding or changing files and folders on mapped client-devices, enable the **Read-only client drive access** policy setting. When adding this setting to a policy, ensure that the Client drive redirection setting is set to **Allowed** and is also added to the policy.

**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.

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
Citrix Virtual Apps and Desktops service

- Default policy settings
- Policy settings reference

Manage

July 8, 2020

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, plus the apps, desktops, and users.

- **Autoscale**: A consistent, high-performance solution to proactively power manage your machines.
- **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. With Citrix virtual loopback, you can 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. As you add Cloud Connectors, VDAs must have current information.
- **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.
- **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. Scale, size, and other configuration considerations are also provided.

• **Delegated administration**: With delegated administration, you can configure the access permissions that all of your administrators need, according to their role in your organization.

• **Configuration logging**: Configuration logging tracks configuration changes and administrative activities.

• **Event logs**: Services within Citrix Virtual Apps and Desktops log the events that occur. Event logs can be used to monitor and troubleshoot operations.

• **Licenses**: You can view Citrix license usage information for this service from the Citrix Cloud console.

---

**Autoscale**

July 27, 2020

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 single-session and multi-session 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...
Citrix Virtual Apps and Desktops service

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 or each half 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-
To define your own schedules, follow the steps below.

1. Select Editschedulesfrom 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 to 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 schedule2 after selecting Monday in schedule1, Monday is automatically cleared in schedule1.
- 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.
- For both RDS and VDI Delivery Groups, you can define the peak times for the days included in a schedule at a granular level of 30 minutes by using the `New-BrokerPowerTimeScheme` PowerShell command. For more information, see [Broker PowerShell SDK commands](#).

**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 to both assigned and 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 Delivery 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:
A machine must meet the following criteria before power policy actions can be applied to it on period transition:

- 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**
  - 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
Citrix Virtual Apps and Desktops service

- 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 roam 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.

© 1999-2020 Citrix Systems, Inc. All rights reserved.
Citrix Virtual Apps and Desktops service

- 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.


**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.

3. **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.
• 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 and is no longer at a baseline load. 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.
• 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 further, but the total spare capacity is at a level above 10,000 in terms of load index.
  – 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 still 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.

Dynamically provision machines with Autoscale

Autoscale provides the capability to create machines and delete them dynamically. You can leverage the capability by using a PowerShell script. The script helps you dynamically scale up or down the number of machines in the Delivery Group based on the current load conditions.

The script offers the following benefits (and more):

- **Reducing storage costs.** Different from Autoscale, which helps reduce your computing costs, the script provides a more cost-effective solution to provision machines.
- **Effectively handling load changes.** The script helps you handle load changes by automatically scaling up or down the number of machines based on the current Delivery Group load.

Download the script

The PowerShell script is available at https://github.com/citrix/Powershell-Scripts/tree/master/XAXD/AutoscaleMcs.

How the script works

**Important:**

- You cannot specify a machine catalog in more than one Delivery Group that is to be managed by the script. In other words, if multiple Delivery Groups share the same machine catalog, the script does not work with any of those Delivery Groups.
Citrix Virtual Apps and Desktops service

You cannot concurrently run the script for the same Delivery Group from multiple locations.

The script works at a Delivery Group level. It measures the load (in terms of load index) and then determines whether to create or delete machines.

Machines created through this script are uniquely tagged (through the ScriptTag parameter) so that they can be identified later. Creating or deleting machines is based on:

- **Maximum percentage load of a Delivery Group.** Specifies the maximum level at which to create machines for Autoscale to address extra loads. When this threshold is exceeded, machines are created in batches to ensure that the current load decreases to or below the threshold.

- **Minimum percentage load of a Delivery Group.** Specifies the minimum level at which to delete machines created through this script that have no active sessions. When this threshold is exceeded, machines created through this script that have no active sessions are deleted.

This script is intended to monitor across a Delivery Group and to create or delete machines when the trigger criterion is met. It executes on a per-run basis. This means that you need to run the script on a regular basis so that it can function as intended. We recommend that you run the script at a minimum interval of five minutes. Doing so improves overall responsiveness.

The script relies on the following parameters to work:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeliveryGroupName</td>
<td>String</td>
<td>X</td>
<td>Name of the Delivery Group to be monitored to determine the current load. You can provide a semicolon-separated list of names. For example: <code>Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile</code>.</td>
</tr>
</tbody>
</table>
## Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XdProfileName</td>
<td>String</td>
<td>X</td>
<td>Name of the profile to use for authenticating to remote servers. For details about authenticating to remote servers using this parameter, see <a href="#">Authentication API</a>.</td>
</tr>
<tr>
<td>HighWatermark</td>
<td>Integer</td>
<td>80</td>
<td>Maximum percentage load (in terms of load index) at which to create machines for Autoscale to address extra loads.</td>
</tr>
<tr>
<td>LowWatermark</td>
<td>Integer</td>
<td>15</td>
<td>Minimum percentage load (in terms of load index) at which to delete machines created through this script that have no active sessions.</td>
</tr>
<tr>
<td>MachineCatalogName</td>
<td>String</td>
<td>X</td>
<td>Name of the machine catalog where machines are to be created.</td>
</tr>
<tr>
<td>MaximumCreatedMachines</td>
<td>Integer</td>
<td>-1</td>
<td>Maximum amount of machines that can be created in a specified Delivery Group. If the value is equal to or less than 0, the script does not process this parameter.</td>
</tr>
<tr>
<td>ScriptTag</td>
<td>String</td>
<td>AutoscaledScripted</td>
<td>Tag that applies to machines created through the script.</td>
</tr>
</tbody>
</table>
By default, the script requires all parameters (except the ScriptTag parameter) the first time it runs. On subsequent runs, only the DeliveryGroupName and the XdProfileName parameters are required. Optionally, you can choose to update the minimum and maximum percentage loads.

Note that you must specify a single Delivery Group the first time you run the script. For example, the script does not work if you use the following PowerShell command to specify two Delivery Groups the first time you run the script:

```
• Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName ‘dg1;dg2’ -XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName ‘cat1’
```

Instead, first specify a single Delivery Group (in this example, dg1) using the following command:

```
• Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName ‘dg1’ -XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName ‘cat1’
```

Then, use the following command to run the script for the second Delivery Group (in this example, dg 2):

```
• Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName ‘dg1;dg2’ -XdProfileName profile
```

**Prerequisites**

To run the script, make sure that these prerequisites are met:

- The machine resides within the same domain where machines are being created.
- Remote PowerShell SDK is installed on that machine. For more information about the Remote PowerShell SDK, see SDKs and APIs.
- Other prerequisites:
  - A Delivery Group to monitor
  - A machine catalog created through Machine Creation Services (MCS) that has an associated provisioning scheme (template)
- An identity pool that is associated with the provisioning scheme
- An event log source to be created so that the script can write information to the Windows Event Log
- A secure client that allows you to authenticate to remote servers

Permissions, recommendations, and notices

When you run the script, keep the following in mind:

- To authenticate to remote servers using the XdProfileName parameter, you need to define an authentication profile by using an API access secure client, created in the Citrix Cloud console. For details, see Authentication API.
- You must have permissions to create and delete machine accounts in Active Directory.
- We recommend that you automate the PowerShell script with Windows Task Scheduler. For details, see Create an automated task using Windows Task Scheduler.
- If you want the script to write information (for example, failures and actions) to the Windows Event Log, you need to first specify a source name using the New-EventLog cmdlet. For example, New-EventLog -LogName Application -Source <sourceName>. You can then view the events in the Application pane of Windows Event Viewer.
- If errors occurred during execution of the script, execute the script manually and then troubleshoot problems by performing script checks.

Authentication API

Before you run the script, you need to define an authentication profile by using an API access secure client. You must create a secure client using the same account under which the script will run.

The secure client must have the following permissions:

- Create and delete machines using MCS.
- Edit machine catalogs (to add and remove machines).
- Edit Delivery Groups (to add and remove machines).

When you create a secure client, make sure that your account has the permissions above because the secure client automatically inherits the permissions from your current account.

To create a secure client, complete these steps:

1. Sign in to Citrix Cloud and then navigate to Identity and Access Management > API Access.
2. Type the name for your secure client and then click Create Client.

To authenticate to remote servers, use the Set-XDCredentials PowerShell command. For example:
Citrix Virtual Apps and Desktops service

- Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>

Create an automated task using Windows Task Scheduler

You can automate the PowerShell script with Windows Task Scheduler. Doing so lets the script run automatically at certain intervals or when certain conditions are met. To execute this script with Windows Task Scheduler, make sure to select **Do not start a new instance** on the **Create Task > Settings** tab. Doing so prevents the Windows Task Scheduler from running a new instance of the script if the script is already running.

Script execution example

See below for an example of executing the script. Note that the script file is invoked multiple times.

In this example, to simulate the load, one session is launched and then terminated.

```powershell
PS C:\Users\Typing\Desktop\Invoke-AutobasicMachineCreation.ps1 -DeliveryGroupName empty -XdProfileName profile -MachineCatalougeName automated -Scripting "emptest" (emptest): Assum default values for emptest. ([1 : 80]).
PS C:\Users\Typing\Desktop\Invoke-AutobasicMachineCreation.ps1 -DeliveryGroupName emptest -XdProfileName profile -MachineCatalougeName automated -Scripting "emptest" (emptest): Assum default values for emptest. ([1 : 80]).
PS C:\Users\Typing\Desktop\Invoke-AutobasicMachineCreation.ps1 -DeliveryGroupName emptest -XdProfileName profile -MachineCatalougeName automated -Scripting "emptest" (emptest): Assum default values for emptest. ([1 : 80]).
PS C:\Users\Typing\Desktop\Invoke-AutobasicMachineCreation.ps1 -DeliveryGroupName emptest -XdProfileName profile -MachineCatalougeName automated -Scripting "emptest" (emptest): Process of provisioning an emptest (. emptest): began provisioning of 1 machines to emptest). Monitoring task (ca2cded-3f0-8f2-d2-f7f2535252f0) is complete. 0 created. 0 failed to create.
PS C:\Users\Typing\Desktop\Invoke-AutobasicMachineCreation.ps1 -DeliveryGroupName emptest -XdProfileName profile -MachineCatalougeName automated -Scripting "emptest" (emptest): Process of provisioning an emptest (. emptest): began provisioning of 1 machines to emptest). Monitoring task (ca2cded-3f0-8f2-d2-f7f2535252f0) is complete. 1 created. 0 failed to create.
PS C:\Users\Typing\Desktop\Invoke-AutobasicMachineCreation.ps1 -DeliveryGroupName emptest -XdProfileName profile -MachineCatalougeName automated -Scripting "emptest" (emptest): Process of provisioning an emptest (. emptest): began provisioning of 1 machines to emptest). Monitoring task (ca2cded-3f0-8f2-d2-f7f2535252f0) is complete. 0 created. 0 failed to create.
PS C:\Users\Typing\Desktop\Invoke-AutobasicMachineCreation.ps1 -DeliveryGroupName emptest -XdProfileName profile -MachineCatalougeName automated -Scripting "emptest" (emptest): Process of provisioning an emptest (. emptest): began provisioning of 1 machines to emptest). Monitoring task (ca2cded-3f0-8f2-d2-f7f2535252f0) is complete. 1 created. 0 failed to create.
PS C:\Users\Typing\Desktop\Invoke-AutobasicMachineCreation.ps1 -DeliveryGroupName emptest -XdProfileName profile -MachineCatalougeName automated -Scripting "emptest" (emptest): Process of provisioning an emptest (. emptest): began provisioning of 1 machines to emptest). Monitoring task (ca2cded-3f0-8f2-d2-f7f2535252f0) is complete. 0 created. 0 failed to create.
```

Troubleshooting checklist for the script

The script writes information (for example, errors and actions) to the Windows Event Log. The information helps you troubleshoot issues you experience when executing the script. It might be helpful to keep the following troubleshooting checklist in mind:

- Failure to communicate with remote servers. Possible actions:
  - Verify your connection to the server.
  - Verify that the API key you use is valid.
- Failure to create machines. Possible actions:
Citrix Virtual Apps and Desktops service

- Verify that the user account running the script has sufficient permissions to create user accounts in the domain.
- Verify that the user who created the API key has sufficient permissions to use MCS to provision machines.
- Verify the validity of the machine catalog (that is, its image still exists and is in good state).
• Failure to add machines to a machine catalog or a Delivery Group. Possible action:
  - Verify that the user who created the API key has sufficient permissions to add and remove machines to and from machine catalogs and Delivery Groups.

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/.

New-BrokerPowerTimeScheme

Creates a new BrokerPowerTimeScheme for a Delivery Group. For more information about this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/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 example:
  
  - 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:

- 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

**Good to know**

Autoscale works at a Delivery Group level. It is configured on a per-Delivery Group basis. It powers 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.
Citrix Virtual Apps and Desktops service

- 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.** To overcome this bottleneck, you can use a PowerShell script to create machines and delete them dynamically. For more information, see Dynamically provision machines with Autoscale.

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

August 18, 2020

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 has 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 CSV or HTML report containing configuration log data, use PowerShell cmdlets for the ConfigLogging Service in the Citrix Virtual Apps and Desktops Remote PowerShell SDK. For details, see:

- Export-LogReportCsv
- Export-LogReportHtml

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
Citrix Virtual Apps and Desktops service

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 or HTML report of logged operations using PowerShell cmdlets only. In the on-premises product, reports can be generated from Studio or PowerShell.
- You cannot delete configuration log content.

**Delegated administration**

June 24, 2020

**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.
Citrix Virtual Apps and Desktops service

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.

For information about displaying the list of administrators and defining access permissions, see 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 can access 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 a scope of London can see all global objects and any objects in the London scope (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>

**Note:**

Custom access administrator roles (except Cloud Administrator and Help Desk Administrator) are not available for Citrix Managed Desktops, Virtual Apps Essentials, and Virtual Desktops Essentials.

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). For 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

To add administrators, follow the guidance 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:
Citrix Virtual Apps and Desktops service

1. After signing in to 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 current administrators in the account.

3. Click **Add administrators from**, and then select your authentication method. Enter the person’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 control 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. Names 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 select 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.
Scopes cannot be created for Full access administrators, nor can they be created for Cloud Administrators or Help Desk Administrators. Those administrators always have the All scope.

Rules for creating and managing scopes:

- Scope names can contain up to 64 Unicode characters. 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 into 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 select 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. Select 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 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, 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.
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...

- **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 administrator 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

July 14, 2020

Local Host Cache 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 60 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 resource location must have a customer-deployed on-premises StoreFront. Local Host Cache works only in resource locations containing an on-premises StoreFront. Verify that the resource location contains a local StoreFront that points to all the Cloud Connectors in that resource location.

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 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, times, and types of recent activity by users.
How it works

During normal operations

- The Brokering Principal (also known as the Citrix Remote Broker Provider Service) on a Cloud Connector accepts connection requests from StoreFront. The Brokering Principal 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 minute to see if any configuration changes were 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 occurred since the previous check, the CSS synchronizes (copies) information to a secondary broker on the Cloud Connector (The secondary broker is also known as the High Availability Service, or HA broker, as shown in the preceding figure).

All configuration data is copied, not just items that changed since the previous check. The CSS imports the configuration data into a Microsoft SQL Server Express LocalDB database on the Cloud Connector. This database is referred to as the Local Host Cache database. The CSS ensures that the information in the Local Host Cache database matches the information in the site database in Citrix Cloud. The Local Host Cache database is re-created each time synchronization occurs.

Microsoft SQL Server Express LocalDB (used by the Local Host Cache database) is installed automat-
ically when you install a Cloud Connector. The Local Host Cache database cannot be shared across Cloud Connectors. You do not need to back up the Local Host Cache 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**

![Citrix Virtual Apps and Desktops service diagram]

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 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 running on other Cloud Connectors in the resource location. The secondary brokers communicate with each other on a separate channel. Those brokers use an alphabetical list of FQDN names of the machines they’re running on to determine (elect) which secondary broker will broker 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 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 broker, the restart has no impact.
- If that Cloud Connector is the elected 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.

**What is unavailable during an outage, and other differences**

There is no time limit imposed for operating in outage mode. However, if the outage is due to loss of Citrix Cloud connectivity from their resource location, Citrix recommends restoring connectivity from the resource location as quickly as possible.

During an outage:

- You cannot use Studio or run PowerShell commands.
- Monitoring data is not sent to Citrix Cloud during an outage. So, the Monitor functions (Director) do not show activity from an outage interval.
Citrix Virtual Apps and Desktops service

- 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.
- Server-hosted applications and desktop users might 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 broker. Launches across zones (from a broker in one zone to a VDA in a different zone) are not supported during an outage.
- If a site database outage occurs before a scheduled restart begins for VDAs in a delivery group, the restarts begin when the outage ends. This scenario can have unintended results. For more information, see Scheduled restarts delayed due to database outage.

**StoreFront requirement**

Each resource location must have a customer-deployed on-premises StoreFront. Local Host Cache works only in resource locations containing an on-premises StoreFront. It does not support Workspace.

**Resource availability**

You can ensure the availability of resources (apps and desktops) during an outage in two ways:

- Publish the resources in every resource location in your deployment.
- Publish the resources to at least one resource location. Then use the following procedure to enable the advanced health check feature in each StoreFront store.

  1. Upgrade the StoreFront installation in each resource location to minimum version 1912 CU1. For guidance, see the StoreFront documentation.
  2. For each StoreFront store, enable the advanced health check option. In the store’s `web.config` file, under `farmsets`, add `advancedHealthCheck="on"`.

    For example:
3. After you update the file, manually restart IIS. Repeat the web.config file update and IIS restart for other stores.

**Application and desktop support**

Local Host Cache works only with customer-deployed StoreFront. It does not support Workspace.

Local Host Cache supports server-hosted applications and desktops, and static (assigned) desktops.

Local Host Cache supports desktop VDAs in pooled delivery groups, as follows.

- 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 command.

  ```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.

**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, this Local Host Cache is an entirely different implementation.
Citrix Virtual Apps and Desktops service

This implementation has significant improvements, is more robust, is more immune to corruption, and requires less maintenance.

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 Microsoft SQL Server Express 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 SQL Server Express 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 all the Cloud Connectors in that resource location.
- Ensure that synchronization imports complete successfully. Check the event logs.
- Ensure that the Local Host Cache database 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`.
  - Verify that `HaDatabaseName.mdf` and `HaDatabaseName_log.ldf` 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 the Cloud Connectors back into normal mode. This can take approximately 15 minutes.

Event logs

Event logs indicate when synchronizations and outages occur. In event viewer logs, outage mode is referred to as HA mode.

Config Synchronizer Service

During normal operations, the following events can occur when the CSS imports the configuration data into the Local Host Cache database using the Local Host Cache broker.
• 503: The Citrix Config Sync Service received an updated configuration. This event occurs each time an updated configuration is received from Citrix Cloud. It indicates the start of the synchronization process.
• 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 is 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 broker 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

This service is also known as the Local Host Cache broker.

• 3502: An outage occurred and the Local Host Cache broker is performing broker operations.
• 3503: An outage was resolved and normal operations have resumed.
• 3504: Indicates which Local Host Cache broker is elected, plus other Local Host Cache 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 registration storms).
• 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, create and set OutageModeForced as REG_DWORD to 1. This setting instructs the Local Host Cache broker to enter outage mode, regardless of the state of the connection to Citrix Cloud. Setting the value to 0 takes the Local Host Cache broker out of outage mode.

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 Local Host Cache database 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 following 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
```

More information

See [Scale and size considerations for Local Host Cache](#) for information about:

- Testing methodologies and results
- RAM size considerations
- CPU core and socket configuration considerations
- Storage considerations

Copied!
Failed!

Scale and size considerations for Local Host Cache

July 21, 2020

This article contains detailed information about Local Host Cache testing, and considerations when configuring your deployment. For general information about Local Host Cache and how it works, see [Local Host Cache](#).
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 article assumes that the reader can set up and configure a Citrix Cloud environment according to recommended standards, with a minimum of three Cloud Connectors.

Local Host Cache supports only on-premises StoreFront in each resource location or zone.

While outage mode is active, if the elected Cloud Connector that brokers the sessions has an outage, the second Cloud Connector becomes the elected High Availability Service. After the election, the second Cloud Connector takes over to broker the sessions. The Local Host Cache feature uses only one socket for multi-core CPUs for the Cloud 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 reregister 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 reregister 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 reregister 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 then 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 Cloud 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 logon 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 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 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
### 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>Authenticate</td>
<td>135 ms</td>
</tr>
<tr>
<td>Enumerate</td>
<td>317 ms</td>
</tr>
<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 Cloud Connector is performing the brokering, whereas normally the StoreFront traffic traverses through the Cloud 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>
</tbody>
</table>
Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Session launch test</th>
<th>Average CPU %</th>
<th>Peak CPU %</th>
</tr>
</thead>
<tbody>
<tr>
<td>20,000 server VDA sessions</td>
<td>Connector 1</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Connector 2</td>
<td>23</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></td>
<td>Connector 2</td>
<td>0.8</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 Cloud Connectors to have identical Cloud 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) 471</td>
<td>687</td>
</tr>
<tr>
<td></td>
<td>Connector 2 1210</td>
<td>1227</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 12.9</td>
<td>29.5</td>
<td></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>
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.
- Cloud Connector 2 did not have any meaningful metrics, as it was not the elected High Availability Service.

VDA reregistration time while switching to Local Host Cache

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

<table>
<thead>
<tr>
<th>Number of VDAs</th>
<th>reregistration time</th>
</tr>
</thead>
<tbody>
<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>Reregistration time to elected</td>
<td>500</td>
<td>~8 minutes</td>
</tr>
<tr>
<td>High Availability Service</td>
<td></td>
<td></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>Reregistration time to Citrix</td>
<td>500</td>
<td>~5.5 minutes</td>
</tr>
<tr>
<td>Delivery Controller</td>
<td></td>
<td></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 reregister 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 Availability 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>Local Host Cache outage mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20,000 server VDA sessions</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>

© 1999-2020 Citrix Systems, Inc. All rights reserved.
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 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**

© 1999-2020 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 Cloud 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 reregistration time while switching to Local Host Cache**

During a Delivery Controller outage, the 1000 workstation VDAs must reregister with the elected Local Host Cache broker. The reregistration 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 Cloud 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 Cloud 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 reregistration 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

**RAM size considerations**

SQL Server Express LocalDB can use up to 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 (the Local Host Cache broker) can use up to 1 GB of RAM if an outage lasts 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. Consider increasing 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 than memory allocation. This CPU overhead is observed only during the outage period when the database is unreachable and the Local Host Cache broker is active.

While SQL Server Express 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
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 Local Host Cache database grows. For example, during a logon/logoff test running at 10 logons per second, the database grew by 1 MB every 2 to 3 minutes. When normal operation resumes, the Local Host Cache database is recreated when a configuration change is detected. The Local Host Cache broker must have sufficient space on the drive where the Local Host Cache database is installed to allow for the database growth during an outage. Local Host Cache also incurs more I/O during an outage: approximately 3 MB of writes per second, with several hundred thousand reads.

**Virtual IP and virtual loopback**

April 7, 2020

**Important:**

Windows 10 Enterprise multi-session doesn’t support Remote Desktop IP Virtualization (Virtual IP) and we don’t support Virtual IP nor virtual loopback on Windows 10 Enterprise multi-session.

These features are valid only for supported Windows server machines. They do not apply to Windows desktop OS machines.

The Microsoft virtual IP address feature provides a published application with a unique dynamically-assigned IP address for each session. The Citrix virtual loopback feature allows you to configure applications that depend on communications with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.*).

Certain applications, such as CRM and Computer Telephony Integration (CTI), use an IP address for addressing, licensing, identification, or other purposes and thus require a unique IP address or a loopback address in sessions. Other applications may bind to a static port, so attempts to launch additional instances of an application in a multiuser environment will fail because the port is already in use. For such applications to function correctly in a Citrix Virtual Apps environment, a unique IP address is required for each device.

Virtual IP and virtual loopback are independent features. You can use either or both.

Administrator action synopsis:
Citrix Virtual Apps and Desktops service

- To use Microsoft virtual IP, enable and configure it on the Windows server. (Citrix policy settings are not needed.)
- To use Citrix virtual loopback, configure two settings in a Citrix policy.

**Virtual IP**

When virtual IP is enabled and configured on the Windows server, each configured application running in a session appears to have a unique address. Users access these applications on a Citrix Virtual Apps server in the same way they access any other published application. A process requires virtual IP in either of the following cases:

- The process uses a hard-coded TCP port number
- The process uses Windows sockets and requires a unique IP address or a specified TCP port number

To determine if an application needs to use virtual IP addresses:

1. Obtain the TCPView tool from Microsoft. This tool lists all applications that bind specific IP addresses and ports.
2. Disable the Resolve IP Addresses feature so that you see the addresses instead of host names.
3. Launch the application and use TCPView to see which IP addresses and ports are opened by the application and which process names are opening these ports.
4. Configure any processes that open the IP address of the server, 0.0.0.0, or 127.0.0.1.
5. To ensure that an application does not open the same IP address on a different port, launch an additional instance of the application.

**How Microsoft Remote Desktop (RD) IP virtualization works**

- Virtual IP addressing must be enabled on the Microsoft server.

  For example, in a Windows Server 2008 R2 environment, from Server Manager, expand Remote Desktop Services > RD Session Host Connections to enable the RD IP Virtualization feature and configure the settings to dynamically assign IP addresses using the Dynamic Host Configuration Protocol (DHCP) server on a per-session or per-program basis. See the Microsoft documentation for instructions.

- After the feature is enabled, at session start-up, the server requests dynamically-assigned IP addresses from the DHCP server.

- The RD IP Virtualization feature assigns IP addresses to remote desktop connections per-session or per-program. If you assign IP addresses for multiple programs, they share a per-session IP address.
Citrix Virtual Apps and Desktops service

- After an address is assigned to a session, the session uses the virtual address rather than the primary IP address for the system whenever the following calls are made: bind, closesocket, connect, WSACreate, WSASocket, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyaddr, getnameinfo, getaddrinfo

When using the Microsoft IP virtualization feature within the Remote Desktop session hosting configuration, applications are bound to specific IP addresses by inserting a “filter” component between the application and Winsock function calls. The application then sees only the IP address it should use. Any attempt by the application to listen for TCP or UDP communications is bound to its allocated virtual IP address (or loopback address) automatically, and any originating connections opened by the application originate from the IP address bound to the application.

In functions that return an address (such as GetAddrInfo(), which is controlled by a Windows policy), if the local host IP address is requested, virtual IP looks at the returned IP address and changes it to the virtual IP address of the session. Applications that attempt to get the IP address of the local server through such name functions see only the unique virtual IP address assigned to that session. This IP address is often used in subsequent socket calls, such as bind or connect. For more information about Windows policies, see RDS IP Virtualization in Windows Server.

Often, an application requests to bind to a port for listening on the address 0.0.0.0. When an application does this and uses a static port, you cannot launch more than one instance of the application. The virtual IP address feature also looks for 0.0.0.0 in these call types and changes the call to listen on the specific virtual IP address, which enables more than one application to listen on the same port on the same computer because they are all listening on different addresses. The call is changed only if it is in an ICA session and the virtual IP address feature is enabled. For example, if two instances of an application running in different sessions both try to bind to all interfaces (0.0.0.0) and a specific port (such as 9000), they are bound to VIPAddress1:9000 and VIPAddress2:9000 and there is no conflict.

Virtual loopback

Enabling the Citrix virtual IP loopback policy settings allows each session to have its own loopback address for communication. When an application uses the localhost address (default = 127.0.0.1) in a Winsock call, the virtual loopback feature simply replaces 127.0.0.1 with 127.X.X.X, where X.X.X is a representation of the session ID + 1. For example, a session ID of 7 is 127.0.0.8. In the unlikely event that the session ID exceeds the fourth octet (more than 255), the address rolls over to the next octet (127.0.1.0), to the maximum of 127.255.255.255.

A process requires virtual loopback in either of the following cases:

- The process uses the Windows socket loopback (localhost) address (127.0.0.1)
- The process uses a hard-coded TCP port number

Use the virtual loopback policy settings for applications that use a loopback address for interprocess
communication. No additional configuration is required. Virtual loopback has no dependency on Virtual IP, so you do not have to configure the Microsoft server.

- Virtual IP loopback support. When enabled, this policy setting allows each session to have its own virtual loopback address. This setting is disabled by default. The feature applies only to applications specified with the Virtual IP virtual loopback programs list policy setting.
- Virtual IP virtual loopback programs list. This policy setting specifies the applications that use the virtual IP loopback feature. This setting applies only when the Virtual IP loopback support policy setting is enabled.

Related feature

You can use the following registry settings to ensure that virtual loopback is given preference over virtual IP; this is called preferred loopback. However, proceed with caution:

- Use preferred loopback only if both Virtual IP and virtual loopback are enabled; otherwise, you may have unintended results.
- Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Run regedit on the servers where the applications reside.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Name: PreferLoopback, Type: REG_DWORD, Data: 1
- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: <list of processes>

Sessions

June 30, 2020

Maintaining session activity is critical to providing the best user experience. Losing connectivity due to unreliable networks, highly variable network latency, and range limitations of wireless devices can lead to user frustration. Being able to move quickly between workstations and access the same set of applications each time they log on is a priority for many mobile workers such as health-care workers in a hospital.
The features described in this article optimize the reliability of sessions, reduce inconvenience, downtime, and loss of productivity; using these features, mobile users can roam quickly and easily between devices.

You can also log a user off of a session, disconnect a session, and configure session prelaunch and linger; see Manage Delivery Groups.

Session reliability

Session Reliability keeps sessions active and on the user’s screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes.

This feature is especially useful for mobile users with wireless connections. For example, a user with a wireless connection enters a railroad tunnel and momentarily loses connectivity. Ordinarily, the session is disconnected and disappears from the user’s screen, and the user has to reconnect to the disconnected session. With Session Reliability, the session remains active on the machine. To indicate that connectivity is lost, the user’s display freezes and the cursor changes to a spinning hourglass until connectivity resumes on the other side of the tunnel. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session Reliability reconnects users without reauthentication prompts.

Citrix Workspace app users cannot override the Controller setting.

You can use Session Reliability with Transport Layer Security (TLS). TLS encrypts only the data sent between the user device and Citrix Gateway.

Enable and configure Session Reliability with the following policy settings:

- The Session reliability connections policy setting allows or prevents session reliability.
- The Session reliability timeout policy setting has a default of 180 seconds, or three minutes. Although you can extend the amount of time Session Reliability keeps a session open, this feature is designed for user convenience and therefore does not prompt the user for reauthentication. As you extend the amount of time a session is kept open, chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.
- Incoming session reliability connections use port 2598, unless you change the port number in the Session reliability port number policy setting.
- If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, use the Auto Client Reconnect feature. You can configure the Auto client reconnect authentication policy setting to prompt users to reauthenticate when reconnecting to interrupted sessions.

If you use both Session Reliability and Auto Client Reconnect, the two features work in sequence. Session Reliability closes, or disconnects, the user session after the amount of time you specify in the
Session reliability timeout policy setting. After that, the Auto Client Reconnect policy settings take effect, attempting to reconnect the user to the disconnected session.

**Auto Client Reconnect**

With the Auto Client Reconnect feature, Citrix Workspace app can detect unintended disconnections of ICA sessions and reconnect users to the affected sessions automatically. When this feature is enabled on the server, users do not have to reconnect manually to continue working.

For application sessions, Citrix Workspace app attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For desktop sessions, Citrix Workspace app attempts to reconnect to the session for a specified period of time, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this period of time is five minutes. To change this period of time, edit this registry on the user device:

```
HKLM\Software\Citrix\ICA Client\Transport\ReconnectRetryMaxTimeSeconds; DWORD; <seconds>
```

where `seconds` is the number of seconds after which no more attempts are made to reconnect the session.

Enable and configure Auto Client Reconnect with the following policy settings:

- **Auto client reconnect**: Enables or disables automatic reconnection by Citrix Workspace app after a connection has been interrupted.

- **Auto client reconnect authentication**: Enables or disables the requirement for user authentication after automatic reconnection.

- **Auto client reconnect logging**: Enables or disables logging of reconnection events in the event log. Logging is disabled by default. When enabled, the server’s system log captures information about successful and failed automatic reconnection events. Each server stores information about reconnection events in its own system log; the site does not provide a combined log of reconnection events for all servers.

Auto Client Reconnect incorporates an authentication mechanism based on encrypted user credentials. When a user initially logs on, the server encrypts and stores the user credentials in memory, and creates and sends a cookie containing the encryption key to Citrix Workspace app. Citrix Workspace app submits the key to the server for reconnection. The server decrypts the credentials and submits them to Windows logon for authentication. When cookies expire, users must reauthenticate to reconnect to sessions.

Cookies are not used if you enable the auto client reconnection authentication setting. Instead, users are presented with a dialog box to users requesting credentials when Citrix Workspace app attempts to reconnect automatically.
For maximum protection of user credentials and sessions, use encryption for all communication between clients and the Site.

Disable Auto Client Reconnect on Citrix Workspace app for Windows by using the icaclient.adm file. For more information, see the documentation for your Citrix Workspace app for Windows version.

Settings for connections also affect Auto Client Reconnect:

- By default, Auto Client Reconnect is enabled through policy settings at the Site level, as described above. User reauthentication is not required. However, if a server’s ICA TCP connection is configured to reset sessions with a broken communication link, automatic reconnection does not occur. Auto Client Reconnect works only if the server disconnects sessions when there is a broken or timed out connection. In this context, the ICA TCP connection refers to a server’s virtual port (rather than an actual network connection) that is used for sessions on TCP/IP networks.
- By default, the ICA TCP connection on a server is set to disconnect sessions with broken or timed out connections. Disconnected sessions remain intact in system memory and are available for reconnection by Citrix Workspace app.
- The connection can be configured to reset or log off sessions with broken or timed-out connections. When a session is reset, attempting to reconnect initiates a new session; rather than restoring a user to the same place in the application in use, the application is restarted.
- If the server is configured to reset sessions, Auto Client Reconnect creates a new session. This process requires users to enter their credentials to log on to the server.
- Automatic reconnection can fail if Citrix Workspace app or the plug-in submits incorrect authentication information, which might occur during an attack or the server determines that too much time has elapsed since it detected the broken connection.

ICA Keep-Alive

Enabling the ICA Keep-Alive feature prevents broken connections from being disconnected. When enabled, if the server detects no activity (for example, no clock change, no mouse movement, no screen updates), this feature prevents Remote Desktop Services from disconnecting that session. The server sends keep-alive packets every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

Important:

ICA Keep-Alive works only if you are not using Session Reliability. Session Reliability has its own mechanisms to prevent broken connections from being disconnected. Configure ICA Keep-Alive only for connections that do not use Session Reliability.

ICA Keep-Alive settings override keep-alive settings that are configured in Microsoft Windows Group Policy.
Enable and configure ICA Keep-Alive with the following policy settings:

- **ICA keep alive timeout:** Specifies the interval (1-3600 seconds) used to send ICA keep-alive messages. Do not configure this option if you want your network monitoring software to close inactive connections in environments where broken connections are so infrequent that allowing users to reconnect to sessions is not a concern.

  The default interval is 60 seconds: ICA Keep-Alive packets are sent to user devices every 60 seconds. If a user device does not respond in 60 seconds, the status of the ICA sessions changes to disconnected.

- **ICA keep alives:** Sends or prevents sending ICA keep-alive messages.

**Workspace control**

Workspace control lets desktops and applications follow a user from one device to another. This ability to roam enables a user to access all desktops or open applications from anywhere simply by logging on, without having to restart the desktops or applications on each device. For example, workspace control can assist health-care workers in a hospital who need to move quickly among different workstations and access the same set of applications each time they log on. If you configure workspace control options to allow it, these workers can disconnect from multiple applications at one client device and then reconnect to open the same applications at a different client device.

Workspace control affects the following activities:

- **Logging on:** By default, workspace control enables users to reconnect automatically to all running desktops and applications when logging on, bypassing the need to reopen them manually. Through workspace control, users can open disconnected desktops or applications, as well as any that are active on another client device. Disconnecting from a desktop or application leaves it running on the server. If you have roaming users who need to keep some desktops or applications running on one client device while they reconnect to a subset of their desktops or applications on another client device, you can configure the logon reconnection behavior to open only the desktops or applications that the user disconnected from previously.

- **Reconnecting:** After logging on to the server, users can reconnect to all of their desktops or applications at any time by clicking Reconnect. By default, Reconnect opens desktops or applications that are disconnected, plus any that are currently running on another client device. You can configure Reconnect to open only those desktops or applications that the user disconnected from previously.

- **Logging off:** For users opening desktops or applications through StoreFront, you can configure the Log Off command to log the user off from StoreFront and all active sessions together, or log off from StoreFront only.

- **Disconnecting:** Users can disconnect from all running desktops and applications at once, without needing to disconnect from each individually.
Workspace control is available only for Citrix Workspace app users who access desktops and applications through a Citrix StoreFront connection. By default, workspace control is disabled for virtual desktop sessions, but is enabled for hosted applications. Session sharing does not occur by default between published desktops and any published applications running inside those desktops.

User policies, client drive mappings, and printer configurations change appropriately when a user moves to a new client device. Policies and mappings are applied according to the client device where the user is currently logged on to the session. For example, if a health care worker logs off from a client device in the emergency room of a hospital and then logs on to a workstation in the hospital's x-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the x-ray laboratory go into effect at the session startup.

You can customize which printers appear to users when they change locations. You can also control whether users can print to local printers, how much bandwidth is consumed when users connect remotely, and other aspects of their printing experiences.

For information about enabling and configuring workspace control for users, see the StoreFront documentation.

**Session roaming**

By default, sessions roam between client devices with the user. When the user launches a session and then moves to another device, the same session is used and applications are available on both devices. The applications follow, regardless of the device or whether current sessions exist. In many cases, printers and other resources assigned to the application also follow.

While this default behavior offers many advantages, it might not be ideal in all cases. You can prevent session roaming using the PowerShell SDK.

Example 1: A medical professional is using two devices, completing an insurance form on a desktop PC, and looking at patient information on a tablet.

- If session roaming is enabled, both applications appear on both devices (an application launched on one device is visible on all devices in use). This might not meet security requirements.
- If session roaming is disabled, the patient record does not appear on the desktop PC, and the insurance form does not appear on the tablet.

Example 2: A production manager launches an application on the PC in his office. The device name and location determine which printers and other resources are available for that session. Later in the day, he goes to an office in the next building for a meeting that will require him to use a printer.

- If session roaming is enabled, the production manager would probably be unable to access the printers near the meeting room, because the applications he launched earlier in his office resulted in the assignment of printers and other resources near that location.
• If session roaming is disabled, when he logs on to a different machine (using the same credentials), a new session is started, and nearby printers and resources will be available.

**Configure session roaming**

To configure session roaming, use the following entitlement policy rule cmdlets with the “SessionReconnection” property. Optionally, you can also specify the “LeasingBehavior” property.

For desktop sessions:

```powershell
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

For application sessions:

```powershell
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Where `value` can be one of the following:

- **Always:** Sessions always roam, regardless of the client device and whether the session is connected or disconnected. This is the default value.
- **DisconnectedOnly:** Reconnect only to sessions that are already disconnected; otherwise, launch a new session. (Sessions can roam between client devices by first disconnecting them, or using Workspace Control to explicitly roam them.) An active connected session from another client device is never used; instead, a new session is launched.
- **SameEndpointOnly:** A user gets a unique session for each client device they use. This completely disables roaming. Users can reconnect only to the same device that was previously used in the session.

The “LeasingBehavior” property is described below.

**Effects from other setting:**

Disabling session roaming is affected by the application limit “Allow only one instance of the application per user” in the application's properties in the Delivery Group.

- If you disable session roaming, then disable the “Allow only one instance ...” application limit.
- If you enable the “Allow only one instance ...” application limit, do not configure either of the two values that allow new sessions on new devices.

**Logon interval**

If a virtual machine containing a desktop VDA closes before the logon process completes, you can allocate more time to the process. The default for 7.6 and later versions is 180 seconds (the default for 7.0-7.5 is 90 seconds).
On the machine (or the master image used in a machine catalog), set the following registry key:

**Key**: HKLM\SOFTWARE\Citrix\PortICA

- **Value**: AutoLogonTimeout
- **Type**: DWORD
- Specify a decimal time in seconds, in the range 0-3600.

If you change a master image, update the catalog.

This setting applies only to VMs with single-session desktop (workstation) VDAs. Microsoft controls the logon timeout on machines with multi-session server VDAs.

Tags

January 14, 2020

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”.

- 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 (VDA101-103).
- 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”: VDA101 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”: VDA102 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 (VDA101-110), 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 (VDA101–105)
- CAD designers in the group can access the apps they need on five machines (VDA106-110)
- Users in the group who need Office applications can access the Office apps on ten machines (VDA101-110)

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.
Citrix Virtual Apps and Desktops service

(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.

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>
</tbody>
</table>
When an application has been added to These machines in the selected Delivery
the Delivery Groups are considered for launch

| Two Application Groups, one with tag Machines that have tag A and tag B; if none are available, then machines that have tag A or tag B |
| restriction A and the other with tag restriction B |
| Two Application Groups, one with tag Machines that have tag A; if none are available, then any machine |
| restriction A and the other with no tag restriction |

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

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

Blog post: How to assign desktops to specific servers.
Zones

April 22, 2020

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,
Citrix Virtual Apps and Desktops service

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.

Zones support Workspace 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
Citrix Virtual Apps and Desktops service

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:
Citrix Virtual Apps and Desktops service

- 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 does (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.
Citrix Virtual Apps and Desktops service

**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, can use session sharing for an application, or a session already running the resource being launched), but that session is on a VDA in a zone other than the preferred zone for the user/application, then the system might create a new session. This action 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. Synchronization 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.
Citrix license usage

March 4, 2020

For information about Citrix license usage, see:

- Monitor license and active usage for cloud services
- Monitor license and active usage for Citrix Virtual Apps and Desktops service

User access

July 10, 2020

There are two primary components that provide access to applications and desktops in a Citrix Virtual Apps and Desktops service deployment:

- **Citrix Workspace**: Citrix Workspace is a complete digital solution that allows you to deliver secure access to the information, apps, and other content that are relevant to a person's role in your organization. Users subscribe to the services you make available and can access them from anywhere, on any device. Citrix Workspace helps you organize and automate the most important details your users need to collaborate, make better decisions, and focus fully on their work.

  There is zero effort to deploy Workspace, and it is kept evergreen by Citrix. Workspace is recommended for new and existing customers, previews, and proofs-of-concept.

- **An on-premises StoreFront**: Customers can also use an existing StoreFront to aggregate applications and desktops in Citrix Cloud. This use case offers greater security, including support for two-factor authentication, and prevents users from entering their password into the cloud service. It also allows customers to customize their domain names and URLs. This deployment type is recommended for any Citrix Virtual Apps and Desktops customers who already have StoreFront deployed.

  See also Local Host Cache and StoreFront.
When users connect from outside the corporate firewall, Citrix Cloud can use Citrix Gateway (formerly NetScaler Gateway) technology to secure these connections with SSL. Citrix Gateway or the Citrix VPX virtual appliance is an SSL VPN appliance that is deployed in the demilitarized zone (DMZ). It provides a single secure point of access through the corporate firewall.

**Using Citrix Workspace**

Access to Workspace is through https://<customername>.cloud.com. If needed, you can customize the <customername> portion of the workspace URL. You can then configure the connectivity for each resource location you want to use, so that end-users can access the resources in their workspace. End-users access their workspace using the latest version of Citrix Workspace app.

For more information about using Workspace, see:

- **Configure workspaces**: For configuring access and customizations.
- **Secure workspaces**: For configuring authentication.
- **Manage your Workspace experience**: For understanding how end-users access their workspace and how it appears.

To provide remote access for end-users through Workspace, you can use either Citrix Gateway service or your own Citrix Gateway:

- **To use the Citrix Gateway service**:

  1. In **Citrix Cloud > Resource Locations**, select **Gateway** for the resource location you want to use.
  2. Select **Gateway Service** and then click **Save**.
  3. In **Citrix Cloud > Workspace Configuration > Service Integrations**, locate the Gateway service and select **Enable** from the ellipsis menu.

- **To use your own Citrix Gateway**:

  1. Set up Citrix Gateway as an ICA Proxy (No authentication or session policies are needed).
  2. Configure a resource location to use Citrix Gateway:

     a) In **Citrix Cloud > Resource Locations**, select **Gateway** for the resource location you want to use.

     b) Select **Traditional Gateway** and enter the external FQDN. Do not add a protocol. Ports are optional. Combination remote and internal access is not supported in Workspace.

  3. Bind Citrix Cloud Connectors as Secure Ticket Authority (STA) servers to Citrix Gateway. For details, see CTX232640.

For more information about the Citrix Gateway service and Citrix Gateway, see **Citrix Gateway**.
Using an on-premises StoreFront

For information about configuring an on-premises StoreFront, see the StoreFront documentation.

One benefit of using an existing StoreFront is that the Citrix Cloud Connector provides encryption of user passwords. The Cloud Connector encrypts credentials using AES-256, using a random-generated one-time key. This key is returned directly to Citrix Workspace app and never sent to the cloud. Citrix Workspace app then supplies it to the VDA during session launch to decrypt the credentials and provide a single sign-on experience into Windows.

- For transport, select HTTP and port 80. The StoreFront machine must be able to directly access the Cloud Connector through the FQDN (fully qualified domain name) provided. The Cloud Connector must be able to reach the Cloud NFuse/STA URL at (https://<customermname>.xendesktop.net/Scripts/wpnbr.dll and ctxsta.dll).
- Add Cloud Connectors as Delivery Controllers for high availability.

External access

To provide external access through Citrix Gateway and on-premises StoreFront:

- Set up Citrix Gateway as usual, with authentication and session policies. See the Citrix Gateway documentation for details.
- Point your on-premises StoreFront store’s Delivery Controllers to the Citrix Cloud Connectors.
- Bind Cloud Connectors as STA servers to Citrix Gateway.
- The Citrix Gateway must use the same STA URLs as StoreFront. If the gateway is not already configured to use the STA of an existing Citrix Virtual Apps and Desktops environment, Cloud Connectors can be used as a STA.

Internal access

To provide internal access through an on-premises StoreFront, point the on-premises StoreFront store’s Delivery Controllers to the Citrix Cloud Connectors.

External and internal access

To provide external and internal access through Citrix Gateway and on-premises StoreFront:

- Set up Citrix Gateway as usual, with authentication and session policies. See the Citrix Gateway documentation for details.
- Bind Cloud Connectors as STA servers to Citrix Gateway.
- Point your on-premises StoreFront store’s Delivery Controllers to the Cloud Connectors.
Local Host Cache and StoreFront

Local Host Cache enables connection brokering operations in a Citrix Virtual Apps and Desktops service deployment to continue when Cloud Connectors cannot communicate with Citrix Cloud.

The Local Host Cache feature works only in resource locations containing a customer-deployed on-premises StoreFront. Local Host Cache does not support Workspace.

Each resource location must have a customer-deployed on-premises StoreFront. Verify that the resource location contains a local StoreFront that points to all the Cloud Connectors in that resource location.

For more information, see Local Host Cache.

Copied!
Failed!

Monitor

March 21, 2019

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:
Citrix Virtual Apps and Desktops service

- 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

August 10, 2020

The Monitor dashboard provides a centralized location to monitor the health and usage of a site.

If there are currently no failures and no failures have occurred in the past 60 minutes, panels stay collapsed. When there are failures, the specific failure panel automatically appears.
Panel Description

**User Connection Failures**  
Connection failures over the last 60 minutes. Click the categories next to the total number to view metrics for that type of failure. In the adjacent table, that number is broken out by delivery groups. Connection failures include failures caused by application limits being reached. For more information on application limits, see Applications.

**Failed Single session OS Machines or Failed Multi-session OS Machines**  
Total failures in the last 60 minutes broken out by delivery groups. Failures broken out by types, including failed to start, stuck on boot, and unregistered. For Multi-session OS machines, failures also include machines reaching maximum load.

**Sessions Connected**  
Connected sessions across all delivery groups for the last 60 minutes.

**Average Logon Duration**  
Log on data for the last 60 minutes. The large number on the left is the average logon duration across the hour. Log on 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.
## Action Description

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View a user’s currently connected machine or session</td>
<td>From the Activity Manager and User Details views, view the user’s currently connected machine or session and a list of all machines and sessions to which this user has access. To access this list, click the session switcher icon in the user title bar. For more information, see Restore sessions.</td>
</tr>
<tr>
<td>View the total number of connected sessions across all delivery groups</td>
<td>From the Dashboard, in the Sessions Connected pane, view the total number of connected sessions across all delivery groups for the last 60 minutes. Then click the large total number, which opens the Filters view, where you can display graphical session data based on selected delivery groups and ranges and usage across delivery groups.</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 Troubleshoot applications.</td>
</tr>
<tr>
<td>View data over a longer period</td>
<td>On the Trends view, select the Sessions tab to drill down to more specific usage data for connected and disconnected sessions over a longer period of time (that is, session totals from earlier than the last 60 minutes). To view this information, click View historical trends.</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 cor-
responding **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.

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.

```powershell
Get-BrokerDesktopGroup | Where-Object {
$_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
$_.PublicationName -eq "\<Name on StoreFront\>"
}).DesktopGroupUid
} | Select-Object -Property Name, Uid
```

**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 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 can 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.

*Note:* This functionality is not available for physical machines or machines using Remote PC Access.

<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>
</tbody>
</table>
## Command Function

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shut Down</strong></td>
<td>Performs an orderly (soft) shutdown of the VM. All running processes are halted individually.</td>
</tr>
<tr>
<td><strong>Force Shutdown</strong></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><strong>Suspend</strong></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><strong>Resume</strong></td>
<td>Resumes a suspended VM and restores its original running state.</td>
</tr>
<tr>
<td><strong>Start</strong></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
Citrix Virtual Apps and Desktops service

maintenance mode.

**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.

*Copied!*  
*Failed!*

**Alerts and notifications**

August 10, 2020

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.
Citrix Virtual Apps and Desktops service

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.

© 1999-2020 Citrix Systems, Inc. All rights reserved.
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
Citrix Virtual Apps and Desktops service

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, contact 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 - 400 ms 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, contact 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
**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.
### Citrix Virtual Apps and Desktops service

<table>
<thead>
<tr>
<th>Alert</th>
<th>Supported Hypervisors</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>
<td>Alert thresholds must be configured in the Hypervisor.</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>
<td>Alert thresholds must be configured in the Hypervisor.</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>
<td>Alert thresholds must be configured in the Hypervisor.</td>
</tr>
<tr>
<td>Disk usage</td>
<td>VMware vSphere</td>
<td>Hypervisor</td>
<td>Disk usage alert threshold is reached or exceeded</td>
<td>Alert thresholds must be configured in the Hypervisor.</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>
<td>Alerts are prebuilt in VMware vSphere. No additional configurations are needed.</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>
<td>Alerts are prebuilt with the Delivery Controller. No additional configurations are needed.</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

August 10, 2020

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. Also, 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 extra 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 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.

```
Get-BrokerDesktopGroup | Where-Object {
  $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
    $_.PublishedName -eq "\<Name on StoreFront\>"  
  }).DesktopGroupUid
}
```
Monitor historical trends across a site

August 10, 2020

The Trends view accesses historical trend information of each site for the following parameters:

- sessions
- connection failures
- machine failures
- logon performance
- load evaluation
- capacity management
- machine usage
- resource utilization
- network analysis for each 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 Citrix Gateway 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 delivery 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 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.
Citrix Virtual Apps and Desktops service

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 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 extra 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 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 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, 1 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.

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.
Monitor Autoscale-managed machines

August 10, 2020

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
Citrix Virtual Apps and Desktops service

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

June 22, 2020

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.

The following actions are available:

- 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
- resetting the user profile
Troubleshoot applications

August 10, 2020

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 in Monitoring policy settings.

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...
Citrix Virtual Apps and Desktops service

- 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.

**Copied!**

**Failed!**

## Application probing

August 10, 2020

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.

**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 only. Monitor does not support Single sign-on (SSO) authentication.
- Ensure that Microsoft .NET Framework version 4.7.2 or later is installed on the endpoint machine where you want to install the Probe Agent.

**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.
Citrix Virtual Apps and Desktops service

- A full administrator user account with the following permissions. Reusing existing user accounts for application probing might log off from 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.

Notes:
- 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.
- Use NetBIOS as the domain name in the user name field. For example, NetBIOS/username.
- App probing supports Citrix Content Collaboration service using Workspace authentication (AD only).
4. On the **Configure To Display Probe Result** tab, enter credentials to access the Citrix Virtual Apps and Desktops service. 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:
Citrix Virtual Apps and Desktops service

- 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 runs 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.

*Copied!*

*Failed!*

### Desktop probing

**August 10, 2020**

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 Win-
dows Version 4.8 or later, or Citrix Workspace app for Windows (formerly Citrix Receiver for Win-
dows) Version 1906 or later. Workspace app for Unified Windows Platform (UWP) is not sup-
ported.
- Monitor and Workspace support the default form-based authentication only. Monitor does not
support Single sign-on (SSO) authentication.
- Ensure that Microsoft .NET Framework version 4.7.2 or later is installed on the endpoint machine
where you want to install the Probe Agent.

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 nor-
mal 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 al-
ready 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.

**Notes:**

- 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.
- Use NetBIOS as the domain name in the user name field. For example, NetBIOS/user-name.
- Desktop probing supports Citrix Content Collaboration service using Workspace authentication (AD only).

4. On the **Configure To Display Probe Result** tab, enter your Monitor credentials. You can find the Customer Name, Client ID, and Secret Key from the API Access page in the Citrix Cloud console.
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**.

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 runs 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.
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.

Copied!
Failed!

Troubleshoot machines

August 10, 2020

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** contains 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. 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>
## Citrix Virtual Apps and Desktops service

### Message Type | Messages in Monitor
---|---
**Error** | RDS licensing has exceeded its grace period.
**Error** | A License Server is not configured for the required OS level with the Per Device Client Access licensing type.
**Error** | The configured License Server is incompatible with the RDS Host OS level with the Per Device Client Access licensing type.
**Warning** | Personal Terminal Server is not a valid RDS licensing type in a Citrix Virtual Apps and Desktops deployment.
**Warning** | Remote Desktop for Administration is not a valid licensing type in a Citrix Virtual Apps and Desktops deployment.
**Warning** | An RDS licensing type is not configured.
**Warning** | The Domain Controller or License Server is unreachable with the Per User Client Access RDS licensing type.
**Warning** | 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.

### Note:
This feature is applicable only for Microsoft RDS CAL (Client Access License).

### PVS target device metrics

You can view the status of PVS target devices for single-session and multi-session OS machines on the **Machine Details** page in Director. Several metrics for **Network**, **Boot**, and **Cache** are available on this panel. These metrics help you monitor and troubleshoot PVS target devices to ensure that they are up and running.
**Network:**

- **Network Bandwidth Utilization:** Average bandwidth utilization across all NICs.
- **Server Reconnect Count:** Number of times the server has reconnected due to network issues or server rebalancing or shutdowns and restarts of the Citrix Provisioning Stream Service.
- **Total UDP Retry Count:** Number of times the provisioning target device has tried to reconnect to the provisioning server using UDP. This metric helps you to know if there are any network issues in the Citrix Provisioning Stream Service (for example, bad switch configurations).

**Boot:**

- **Boot Bytes Read MB:** Bytes read while booting.
- **Boot Bytes Written MB:** Bytes written while booting.
- **Boot From:** Boot medium (vDisk, local disk, and so on).
- **Boot Retry Count:** Number of retries to boot the machine.
- **Boot Time:** Time taken to boot the machine, in seconds. By default, there is a 5 second delay between retries. If this delay grows into double digits, there is a significant increase in boot time. Check your provisioning configuration to resolve this issue.
- **Target Software Version:** Version of the Provisioning target device software.
- **vDisk Name:** vDisk from which the Provisioning target device is booting.

**Cache:**

- **Write Cache Type:** vDisk can be set to different types of cache. For more information, see Knowledge Center article CTX119469.
- **Write Cache Volume Drive Letter:** Drive letter for write cache types involving drives.
- **Write Cache Volume Size MB:** Total configured volume size for write cache.
- **Cache File Size MB:** Current cache file size (cache on device RAM with overflow on hard disk).
- **Ram Cache Usage MB:** Current RAM cache size (cache on device RAM with overflow on hard disk). Use Overflow to disk only if necessary. This metric is useful when setting or optimizing the proper size of RAM cache.
Citrix Virtual Apps and Desktops service

For more information, see Using the Status Tray on a target device.

Provisioning target device metrics is available only on:

- Provisioning machines.
- Provisioning target device version 7.19 and later.
- VDA version 2003 and later.

Note:
Metrics for Server Reconnect Count and UDP Retry Count are available only for Provisioning target version 1912 CU2 and later.

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.

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>

© 1999-2020 Citrix Systems, Inc. All rights reserved.
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

August 10, 2020

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 log on 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 the 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.
   - If the user is 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 https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416(v=technet.10).

Logon scripts

If logon scripts are configured for the session, this is the time taken for the logon scripts to be run.


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, the Profile Load bar displays an increased duration. 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 drill down 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 does not guarantee that problems resulting from the incorrect use of the 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**
Citrix Virtual Apps and Desktops service

- Profile drilldown does not consider redirected folders.
- NTUser.dat files in the root folder might 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 might 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 Interactive Session duration = Desktop Ready Event Timestamp (EventId 1000 on VDA) - User Profile Loaded Event Timestamp (EventId 2 on VDA). Interactive Session has three sub-phases: Pre-userinit, Userinit, and Shell. Hover over the Interactive Session to see a tooltip showing the following:

- subphases
- the time taken for each subphase
- the total cumulative time delay between these subphases
- link to 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 an 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 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 https://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10) in the Microsoft documentation.
InteractiveSession–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.

InteractiveSession–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.

InteractiveSession–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, extra processing occurs that can result in a longer logon duration than the sum. 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 subsecond 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...
**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 is 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.

*Copied!*

*Failed!*

**Diagnose session startup issues**

June 22, 2020

In addition to the logon process phases mentioned in the **Diagnose user logon issues** section, Monitor displays the session startup duration. This duration 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 (EUEN) 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 macOS, 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 a 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 the 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.
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. SSCD 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. For 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)

IFDCD 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 the 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 the 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 can 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 can 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 can 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 the user receives keyboard and mouse control.

**Session Creation VDA Duration (SCVD)**

This time includes miscellaneous delays in session creation on VDA.

*Copied!*
*Failed!*

**Shadow users**

June 22, 2020
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.

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 Enable or Disable features.

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 more 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

April 23, 2020

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.

To send a message to a user, follow these steps:

1. Go to Monitor > Filters > Machines > All Machines.
2. Select a machine to which you want to send a message and click Send Message.
3. Type your message 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

July 1, 2020
Citrix Virtual Apps and Desktops service

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 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 fails.</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 from 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**

June 22, 2020

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 22, 2020

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.
### Citrix Virtual Apps and Desktops service

**Action** | **Description**
--- | ---
End applications or processes that are not responding | Click the Applications tab. Select any application that is not responding and click **End Application**. Similarly, select any corresponding process that is not responding and click **End Process**. Also, end processes that are consuming an unusually high amount of memory or CPU resources, which can make the CPU unusable.

Disconnect the Windows session | Click **Session Control** and then select **Disconnect**. This option is available only for brokered Multi-session OS machines. For non-brokered sessions, the option is disabled.

Log off the user from the session | Click **Session Control** and then select **Log Off**.

To test the session, the user can attempt to log back on to it. You can also shadow the user to more closely monitor this session.

*Copied!
*Failed!*

### Run HDX channel system reports

**June 22, 2020**

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**.

Copied!
Failed!

## Reset a user profile

June 22, 2020

**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. For a Citrix user profile, the profile is already reset by the time the user’s desktop appears. For 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:
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 logon, 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 Profile Management processes the user, but receives a roaming profile command, it is rejected (or the opposite way).

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 necessary.

For Microsoft roaming profiles, Windows creates a new profile, 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.

Failed!

Feature compatibility matrix

August 13, 2020

Citrix Monitor supports three Citrix Virtual Apps and Desktops service editions. They are Premium, Citrix Virtual Apps Advanced Service, and Citrix Virtual Apps and Desktops Advanced Service. Specific Citrix Monitor features, VDA versions, dependent components, and their respective license editions are listed in the following table.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Dependencies - min version required</th>
<th>Premium</th>
<th>Citrix Virtual Apps Advanced Service</th>
<th>Citrix Virtual Apps and Desktops Advanced Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Auto Reconnect</td>
<td>VDA 1906</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Session Startup Duration</td>
<td>VDA 1903</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Desktop Probing</td>
<td>Citrix Probe Agent 1903</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Citrix Profile Management</td>
<td>VDA 1903</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Duration in Profile Load</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Profile Drilldown</td>
<td>VDA 1811</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Dependencies - min version required</td>
<td>Premium</td>
<td>Citrix Virtual Apps Advanced Service</td>
<td>Citrix Virtual Apps and Desktops Advanced Service</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------</td>
<td>---------</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Hypervisor Alerts Monitoring</td>
<td>None</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Application Probing</td>
<td>Citrix Application Probe Agent 1811</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Microsoft RDS License Health</td>
<td>VDA 7.16</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Key RTOP Data Display</td>
<td>VDA 1808</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Export of Filters Data</td>
<td>None</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Interactive Session Drill Down</td>
<td>VDA 1808</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GPO Drill Down</td>
<td>VDA 1808</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Machine Historical Data Available Using OData API</td>
<td>None</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Smart Alert Policies</td>
<td>None</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Health Assistant Link</td>
<td>None</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Interactive Session Drill-down</td>
<td>None</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application Analytics</td>
<td>VDA 7.15</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OData API V.4</td>
<td>None</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Dependencies - min version required</td>
<td>Premium</td>
<td>Citrix Virtual Apps Advanced Service</td>
<td>Citrix Virtual Apps and Desktops Advanced Service</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------</td>
<td>---------</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Shadow Linux VDA Users</td>
<td>VDA 7.16</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Machine Console Access</td>
<td>None</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application Failure Monitoring</td>
<td>VDA 7.15</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application-centric Troubleshooting</td>
<td>VDA 7.13</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Disk Monitoring</td>
<td>VDA 7.14</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GPU Monitoring</td>
<td>VDA 7.14</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Transport Protocol on Session Details Panel</td>
<td>VDA 7.13</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User-friendly Connection and Machine Failure Descriptions</td>
<td>VDA 7.x</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Historical Data Retention</td>
<td>VDA 7.x</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Custom Reporting</td>
<td>VDA 7.x</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Resource Utilization Reporting</td>
<td>VDA 7.11</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Delegated administration and monitoring

### August 14, 2020

Delegated administration uses three concepts: administrators, roles, and scopes. Permissions are
Citrix Virtual Apps and Desktops service

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 in addition to 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>
<tr>
<td>Administrator Role</td>
<td>Permissions in Monitor</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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. 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 the Citrix Cloud menu, go to **Identity and Access Management > Administrators**. Here, when you add or edit the 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.
Data granularity and retention

August 24, 2020

Aggregation of data values

The Monitor Service collects various 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. 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, therefore are exposed as sums over a time period.

Concurrent data evaluation

Your sessions must be overlapping to be considered concurrent. However, when the time interval is 1 minute, all sessions in that minute (whether 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 is no summary data for a partial interval at the beginning (oldest available data) or at the end. When viewing aggregations of a day (Interval=1440), this means that the first and most recent incomplete days have no data. Although raw data might exist for those partial intervals, it is never summarized. Pull the min and max SummaryDate from a particular summary table to determine the earliest and latest aggregate interval for a particular data granularity. 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 in the preceding section. They can be used for historical trends, but raw events might be more current in the state than what has been summarized for trend analysis. Any time-based comparison of summary to raw data must take into account that there is no summary data for partial intervals that might occur or for the beginning and ending of the time period.

- **Missed and latent events.** Metrics that are aggregated into the summary table might be slightly inaccurate if events are missed or latent to the aggregation period. Although the Monitor Service attempts to maintain an accurate current state, it does not go back in time to recompute aggregation in the summary tables for missed or latent events.

- **Connection High Availability.** During connection HA, there are gaps in the summary data counts of current connections, but the session instances are still running in the raw data.

- **Data retention periods.** Data in the summary tables is retained on a different grooming schedule from the schedule for raw event data. Data might be missing because it has been groomed away from summary or raw tables. Retention periods might also differ for different granularities of summary data. Lower granularity data (minutes) is groomed more quickly than higher granularity data (days). If data is missing from one granularity due to grooming, it might 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 might 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:
Citrix Virtual Apps and Desktops service

- $0 < T \leq 30$ days use per-hour granularity
- $T > 31$ days use per-day granularity

Requested data that does not come from aggregated data comes from the raw Session and Connection information. This data tends to grow fast, and therefore has its own grooming setting. Grooming ensures that only relevant data is kept long term. This ensures better performance while maintaining the granularity required for reporting.

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 is stored for a period 2 years for backup and recovery.

<table>
<thead>
<tr>
<th>Setting name</th>
<th>Affected grooming</th>
<th>Default values for Premium (limited to 31 days)</th>
<th>Default values for Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GroomSessionsRetentionDays</td>
<td>90</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Session and Connection records retention after Session termination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>GroomFailuresRetentionDays</td>
<td>90</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>MachineFailureLog and Connection-FailureLog records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>GroomLoadIndexesRetentionDays</td>
<td>90</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>LoadIndex records</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 1999-2020 Citrix Systems, Inc. All rights reserved.
### Setting name

<table>
<thead>
<tr>
<th>Setting name</th>
<th>Affected grooming</th>
<th>Default values for Premium</th>
<th>Default values for Advanced (limited to 31 days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 GroomDeletedRetentionDaysMachine, 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>
<td>7</td>
<td></td>
</tr>
<tr>
<td>5 GroomSummariesDesktopGroupSummary, FailureLogSummary, and LoadIndexSummary records. Aggregated data - daily granularity.</td>
<td>90</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>6 GroomMachineHotfixLogRetentionDaysHotfixes applied to the VDA and Controller machines</td>
<td>90</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td>7 GroomHourlyRetentionDaysAggregated data - hourly granularity</td>
<td>32</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8 GroomApplicationInstanceRetentionDaysApplication Instance history</td>
<td>90</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>9 GroomNotificationLogRetentionDaysNotification Log records</td>
<td>90</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Setting name</td>
<td>Affected grooming</td>
<td>Default values for Premium</td>
<td>Default values for Advanced (limited to 31 days)</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>GroomResourceUsageRawDataRetentionDays</td>
<td>Resource utilization data - raw data</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>GroomResourceUsageMinuteDataRetentionDays</td>
<td>Resource utilization summary data - minute granularity</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>GroomResourceUsageHourDataRetentionDays</td>
<td>Resource utilization summary data - hour granularity</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>GroomResourceUsageDayDataRetentionDays</td>
<td>Resource utilization summary data - day granularity</td>
<td>90</td>
<td>7</td>
</tr>
<tr>
<td>GroomProcessUsageRawDataRetentionDays</td>
<td>Process utilization data - raw data</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>GroomProcessUsageMinuteDataRetentionDays</td>
<td>Process utilization data - minute granularity</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>GroomProcessUsageHourDataRetentionDays</td>
<td>Process utilization data - hour granularity</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>GroomProcessUsageDayDataRetentionDays</td>
<td>Process utilization data - day granularity</td>
<td>30</td>
<td>7</td>
</tr>
<tr>
<td>GroomSessionMetricsDataRetentionDays</td>
<td>Session metrics data</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>GroomMachineMetricDataRetentionDays</td>
<td>Machine metrics data</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Citrix Virtual Apps and Desktops service for Citrix Service Providers

June 24, 2020

This article describes how Citrix Service Providers (CSP) can set up the Virtual Apps and Desktops service for tenant customers in Citrix Cloud. For an overview of the features available for Citrix Partners, see Citrix Cloud for Partners.

---

<table>
<thead>
<tr>
<th>Setting name</th>
<th>Affected grooming</th>
<th>Default values for Premium</th>
<th>Default values for Advanced (limited to 31 days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroomMachineMetricData</td>
<td>summary data</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>GroomApplicationErrorData</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>GroomApplicationFailureData</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Caution:
You cannot modify the values on the Monitor Service database. To change any settings in the database, contact Citrix Support.

Retaining data for long periods has 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 can 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 might be large. Excessively large amounts of data can 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 grows 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 Virtual Apps and Desktops service

Requirements

- You are a Citrix Service Provider partner.
- You have a Citrix Cloud account.
- You have a subscription to the Citrix Virtual Apps and Desktops service.

Limitations and known issues

Limitations

- Tenant name changes take up to 24 hours to apply across all interfaces.
- When creating a new tenant, the email address must be unique.
- Studio filtering by scope (similar to Monitor) is not available. To see the resources attached to a scope, select Administrators in the Studio navigation pane. On the Scopes tab, select the scope and then click Edit Scope in the Action pane.

Known issues

- The customer scope name in Studio shows an internal ID rather than the customer name. You can change the scope name to a friendly name. Select Administrators in the Studio navigation pane. On the Scopes tab, select the scope and then click Edit Scope in the Action pane.
- After scopes are assigned to a resource, you cannot use Studio to remove or unassign them. Those tasks are supported only through PowerShell.
- Studio does not enforce scopes. You are responsible for selecting the appropriate scope when creating machine catalogs, Delivery Groups, and Application Groups.
- When more than 15 scopes are created (auto-created and custom), the Citrix Cloud custom access information for an administrator (Identity and Access Management > Administrators) does not display correctly. Workaround: Limit scopes to 15 or fewer.
- After adding the Citrix Virtual Apps and Desktops service to a customer:
  - You cannot remove it from a customer.
  - You cannot remove the link between the customer and the CSP.

Add a customer

1. Sign in to Citrix Cloud with your CSP credentials. Click Customers in the upper left menu.
2. From the Customer Dashboard, click Invite or Add. Provide the requested information.
3. If the customer does not have a Citrix Cloud account, adding the customer creates a customer account. Adding the customer also automatically adds you as a full access administrator of that customer’s account.
4. If the customer has a Citrix Cloud account:
   a) A Citrix Cloud URL displays, which you copy and send to the customer. For details of this process, see Inviting a customer to connect.
   b) The customer must add you as a full access administrator to their account. See Add administrators to a Citrix Cloud account.

You can add more administrators later and control which customers they can see on the Manage and Monitor dashboards.

Add the Citrix Virtual Apps and Desktops service to a customer

1. Sign in to Citrix Cloud with your CSP credentials. Click Customers in the upper left menu.
2. From the Customer Dashboard, in the ellipsis menu for the customer, select Add Service.
3. In Select a Service to Add, click Virtual Apps and Desktops.
4. Click Continue.

After you complete this procedure, the customer is onboarded to your Citrix Virtual Apps and Desktops service subscription.

When the onboarding completes, a new customer scope is created automatically in the Citrix Virtual Apps and Desktops service. The scope is visible in Studio. This scope is unique to that customer. You can rename the scope, but you cannot delete it.

Use this scope to tailor access for other administrators. For example, let’s say you have ten customers and two administrators. Using the unique scope, you can restrict one administrator’s access to only three of the customers, while the other administrator can access one of those three customers, plus two other customers. For details, see Control administrator access to customers.

Set up a resource location

A resource location holds the machines that deliver apps and desktops for your customers, as well as infrastructure components such as Citrix Cloud Connectors. For details, see Connect to Citrix Cloud.

Set up catalogs and groups to deliver apps and desktops

A catalog is a group of identical virtual machines. When you create a catalog, a master image is used (with other settings) as a template for creating the machines. For details, see Create machine catalogs.

A Delivery Group is a collection of machines selected from one or more machine catalogs. The Delivery Group specifies which users can use those machines, plus the applications and/or desktops available to those users. For details, see Create Delivery 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.

When configuring groups, be sure that:

- The Delivery Group's scope is a subset of the machine catalog's scope. For example, assume the catalog's scope is A and B. The Delivery Group's scope can be either A or B, or A and B.
- The Application Group's scope is a subset of the Delivery Group's scope. For example, assume the Delivery Groups associated with an Application Group have scope A and B. The Application Group's scope can be either A or B, or A and B.

Federated domains

Federated domains enable customer users to use credentials from a domain attached to your resource location to sign in to their workspace. This allows you to provide dedicated workspaces to your customers that customer users can access using a custom workspace URL (for example, customer.cloud.com), while the resource location is still on your Citrix Cloud account. You can provide dedicated workspaces alongside the shared workspace that customers can access using your CSP workspace URL (for example, csppartner.cloud.com). To enable customers to access their dedicated workspace, you add them to the appropriate domains that you manage. After configuring the workspace through Workspace Configuration, customers’ users can sign in to their workspace and access the apps and desktops that you’ve made available.

Add a customer to a domain

1. Sign in to Citrix Cloud with your CSP credentials. Click Customers in the upper left menu.
2. From the Customer Dashboard, select Identity and Access Management in the upper left menu.
3. On the Domains tab, select Manage Federated Domain in the domain’s ellipsis menu.
4. On the Manage Federated Domain card, in the Available customers column, select a customer you want to add to the domain. Click the plus sign next to the customer name. The selected customer now appears in the Federated customers column. Repeat to add other customers. When you’re done, click Apply.

Remove a customer from a domain

When you remove a customer from a domain that you manage, the customer’s users can no longer access their workspaces using credentials from your domain.

1. From the Citrix Cloud menu, select Identity and Access Management, then select Domains.
2. Locate the domain you want to manage and click the ellipsis button. Select **Manage Federated Domain**.
3. From the list of federated customers, locate or search for the customers you want to remove and click the X button. Click **Remove all** to remove all the customers in the list from the domain. The selected customers move to the list of available customers.
4. Click **Apply**.
5. Review the customers you selected and select **Remove Customers**.

**Control administrator access to customers**

You can control administrator access to customers by using the unique scope that was created when you added the Citrix Virtual Apps and Desktops service to the customer. You can configure access when you add an administrator or later.

To learn about restricting access using roles and scopes in the Citrix Virtual Apps and Desktops service, see [Delegated administration](#).

**Add an administrator with restricted access**

1. Sign in to Citrix Cloud with your CSP credentials. Click **Customers** in the upper left menu.
2. From the Customer Dashboard, select **Identity and Access Management** in the upper left menu.
3. On the **Administrators** tab, click **Add Administrators From**, and then select **Citrix Identity**.
4. Type the email address of the person you’re adding as an administrator, and then click **Invite**.
5. Configure the appropriate access permissions for the administrator. Citrix recommends selecting **Custom access**, unless you want the administrator to have management control of Citrix Cloud and all of the subscribed services.
6. After selecting **Custom access**, select one or more role and scope pairs for the Virtual Apps and Desktops service, as needed. Be sure to enable only entries that contain the unique scope that was created for the customer.
7. When you’re done selecting role and scope pairs, click **Send Invite**.

When the administrator accepts the invitation, they have the access that you assigned.

**Edit delegated administration permissions for administrators**

1. Sign in to Citrix Cloud with your CSP credentials. Click **Customers** in the upper left menu.
2. From the Customer dashboard, select **Identity and Access Management** in the upper left menu.
3. On the **Administrators** tab, select **Edit Access** from the ellipsis menu for the administrator.
4. Select and clear role and scope pairs for the Virtual Apps and Desktops service, as needed. Be sure to enable only entries that contain the unique scope that was created for the customer.

5. Click Save.

**View customer administrators and their assigned roles and scopes**

1. Sign in to Citrix Cloud with your CSP credentials. Click Customers in the upper left menu.
2. From the Customer Dashboard, select My Services > Virtual Apps and Desktops in the upper left menu.
3. In the Citrix Virtual Apps and Desktops service, click the Manage tab, if it isn’t already selected.
4. Click Configuration > Administrators in the navigation pane.

Information is available on three tabs:

- The **Administrators** tab lists the administrators that have been created, plus their roles and scopes.
- The **Roles** tab lists all roles. To view role details, select the role in the middle pane. The lower portion of that 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.
- The **Scopes** tab lists all the scopes, including those generated for customers of Citrix partners.

**Configure workspaces**

The customer has their own workspace with a unique customer.cloud.com URL. This is where the customer’s users access their published apps and desktops.

The workspace URL is displayed in two places:

- From the Customer dashboard, select Workspace Configuration from the menu in the upper left menu.
- From the Citrix Virtual Apps and Desktops service Welcome page (the Overview tab), the workspace URL appears at the bottom of the page.

You can change access and authentication to a workspace. You can also customize the workspace appearance and preferences. For details, see the following articles:

- Configure workspaces
- Secure workspaces
Monitor a customer’s service

The **Monitor** dashboard in a CSP environment is essentially the same as a non-CSP environment. See **Monitor** for details.

By default, the **Monitor** dashboard displays information about all customers. To display information about one customer, use **Select Customer**.

Keep in mind that the ability to see Monitor displays for a customer is controlled by the administrator’s configured access. The access must include a role and scope pair that includes the customer’s unique scope.

If you used built-in roles to configure access: The built-in roles control whether the administrator can see the **Manage** and **Monitor** displays. If you select only role and customer-scope pairs that do not include **Monitor** tab visibility, that administrator won’t see the **Monitor** tab for any selected customers. For example, if you give an administrator only **Read Only Administrator,customerABC** access, that administrator won’t see the **Monitor** tab for customer ABC, because read only administrators don’t have access to Monitor displays.

**Citrix Gateway service**

May 12, 2020

Citrix Gateway provides users with secure VPN access to Citrix Virtual Apps and Desktops applications.

The Citrix Gateway service enables secure, remote access to those applications, without having to deploy Citrix Gateway in the DMZ or reconfigure your firewall. The infrastructure overhead of using Citrix Gateway moves to Citrix Cloud.

For more information about the Citrix Gateway service, see the [product documentation](#). That content includes how to enable the service and known issues for the version you’re using.

Citrix ADC is an application delivery controller that analyses application-specific traffic to distribute, optimize, and secure Layer 4-Layer 7 (L4–L7) network traffic intelligently for web applications. The Citrix ADC VPX virtual appliance can be hosted on various virtualization and cloud platforms. For details, see [Deploy a Citrix ADC VPX instance](#).

© 1999-2020 Citrix Systems, Inc. All rights reserved.
Citrix Virtual Apps and Desktops service

SDKs and APIs

August 11, 2020

Citrix Virtual Apps and Desktops Remote PowerShell SDK

The Remote PowerShell SDK automates complex and repetitive tasks. It provides the mechanism to set up and manage the Citrix Virtual Apps and Desktops service environment without using the Studio user interface.

- Cmdlet details are provided in Citrix Virtual Apps and Desktops SDK.
- The supported snap-ins are listed in Limitations. That section also lists the cmdlets that are disabled in this SDK.

How this SDK differs from the SDK for customer-managed deployments

In a Citrix Virtual Apps and Desktops deployment that is 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 PowerShell SDK does 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 PowerShell SDK. When running in the resource location, the Remote PowerShell SDK accesses the control plane as if it is local. This provides 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 remain 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 PowerShell SDK calls. If this cmdlet is not explicitly run, it is called by the first PowerShell SDK cmdlet.

Install and use the Remote PowerShell SDK

Requirements:
Citrix Virtual Apps and Desktops service

- Ensure that PowerShell 3.0 or later is available on the machine.
- The SDK installer downloads and installs .NET Framework 4.8 if it (or a later supported version) is not already installed.
- If the machine already has the Citrix Virtual Apps and Desktops 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.
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 PowerShell 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 snap-ins: asnp citrix.*.
- You can explicitly authenticate by using the Get-XdAuthentication cmdlet. Or, run your first Citrix Virtual Apps and Desktops PowerShell SDK command, which prompts 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 running PowerShell SDK cmdlets or PowerShell 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.

To uninstall the Remote PowerShell SDK, 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.

```powershell
1 $users = ”xd.local\Domain Users”
2 $TSVDACatalogName = ”TSVDA”
3 $TSVDADGName = ”TSVDA”
```
$TSVDAMachineName = "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 $TSVDAMachineName
    -CatalogUid $catalog.uid

#Create new desktops & applications delivery group

$dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
    $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession"
    -DeliveryType DesktopsAndApps -Description $TSVDADGName

#Create notepad application

New-BrokerApplication -ApplicationType HostedOnDesktop -Name "Notepad"
    -CommandLineExecutable "notepad.exe" -DesktopGroup $dg

#Assign users to desktops and applications

New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid $dg.Uid
    -IncludedUsers $brokerUsers -description $TSVDADGName

New-BrokerAccessPolicyRule -Name $TSVDADGName -
    IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
    DesktopGroupUid $dg.Uid -AllowedProtocols (@"HDX", "RDP")

New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
    DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName

#Add machine to delivery group

Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
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.

After authentication, remote access remains valid in the current PowerShell session for 24 hours. After this time, you must enter your credentials.

The Remote PowerShell 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 Citrix 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
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
Citrix Virtual Apps and Desktops service

- 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
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
Citrix Virtual Apps and Desktops service

- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- 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:**

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
Citrix Virtual Apps and Desktops service

- 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:**

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
Citrix Virtual Apps and Desktops service

- 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 service discovery module for App-V packages and servers**

The Citrix Virtual Apps and Desktops service can deliver applications contained in App-V packages to your endpoints using the single admin management method (accessing packages from a network share), or using the dual admin management method (accessing packages from a Microsoft App-V Management Server).

The process of registering App-V packages, Microsoft App-V Management, and Publishing Servers with the Application Library using the Citrix Virtual Apps and Desktops service is slightly different from registering packages using an on-premises deployment. However, the process of assigning applications to users and launching them on a user’s endpoint is identical.
The service management console in Citrix Cloud cannot view files in a resource location. Also, it cannot directly discover App-V packages or Microsoft App-V servers in your infrastructure. The discovery module provides functions that discover App-V package information in your on-premises infrastructure and uploads the package information to your Virtual Apps and Desktops service. Package information includes App-V packages, Microsoft App-V servers, and the apps that the packages contain.

The discovery module uses the Virtual Apps and Desktops Remote PowerShell SDK. It can discover package information from either a network share or a Microsoft App-V Management Server. You use the discovery module on a machine in your resource location.

Prerequisites for using the discovery module:

- Verify that PowerShell 3.0 or later is available on the machine.
- Verify that the Citrix Virtual Apps and Desktops Remote PowerShell SDK is installed on the machine.
- Verify that you have access to the network share containing the App-V packages.
- Verify that you have access to the server where the Citrix Cloud Connectors are installed and the Microsoft App-V Management Server is hosted.

Add or remove App-V packages in Citrix Cloud

The procedures below are valid for adding App-V packages from network shares (single admin management) and for adding all published App-V packages from the Microsoft App-V Management Server (dual admin management). If you use the dual admin management method, you must manage the added App-V packages just like you do when using the single admin management method.

Add App-V packages to the Application Library in Citrix Cloud

**Step 1: Download the discovery module**


**Note:**

This file is also provided on the Citrix Virtual Apps and Desktops ISO in Support\Tools\Scripts where you can copy it locally or reference it directly from the CD drive.

**Step 2: Verify that the Virtual Apps and Desktops Remote PowerShell SDK is installed on your machine**
**Step 3: Navigate to the folder containing the discovery module**

In the PowerShell window, type the full path of the folder containing the discovery module and then press **Enter**.

**Step 4: Import the discovery module**


**Step 5: Add the App-V packages to Citrix Cloud**

After importing the module, add the App-V packages to the Application Library in Citrix Cloud by using either of the methods described below.

To add App-V packages from a network share, use the following command in the PowerShell window: `Import-AppVPackageToCloud`. For example: `Import-AppVPackageToCloud -PackagePath \AppVSrv\share\Notepad++.appv`

**Note:**

For more information about using the command, type `Get-Help Import-AppVPackageToCloud` in the PowerShell window to get the help information.

To add App-V packages from a Microsoft App-V Management Server, use the following command in the PowerShell window: `Import-AppVPackagesFromManagementServerToCloud`. For example: `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVMngSrv.domain.local`

**Note:**

- This command imports all published App-V packages from the Microsoft App-V Management Server to Citrix Cloud.
- After adding the App-V packages to Citrix Cloud, you must manage them like you do using the single admin management method.
- For more information about using the command, type `Get-Help Import-AppVPackagesFromManagementServerToCloud` in the PowerShell window to get the help information.

**Step 6: Sign in with your Citrix Cloud credentials**

After the Citrix Cloud window appears, enter your Citrix Cloud credentials and then click **Sign In**. When prompted, select the target customer. After the script executes successfully, the App-V packages are added to the Application Library in Citrix Cloud.
**Citrix Virtual Apps and Desktops service**

**Remove an App-V package from the Application Library in Citrix Cloud**

To remove an App-V package from the Application Library in Citrix Cloud, see Remove an App-V package from the Application Library in on-premises deployments.

**High-level PowerShell functions**

The module contains the following high-level functions that 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.


  Discovers Microsoft App-V Management and Publishing Servers and imports the content to the Application Library. This cmdlet imports all the packages managed using Microsoft App-V Management Server and related information. Servers can be added and removed through PowerShell.

  **Note:** This cmdlet adds App-V packages in dual admin mode. Only App-V packages that are published on the Microsoft App-V Management Server, and which have AD groups added, are imported. If you make changes to the Microsoft App-V Management Server, rerun this cmdlet to synchronize the Application Library with the Microsoft App-V Management Server.


  Removes the Microsoft App-V Management and Publishing Servers added to Application Library.
Note:
This cmdlet removes the specified Microsoft App-V Management and Publishing Servers, plus all the associated App-V packages.

Run the discovery module for App-V packages and servers 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 PowerShell SDK command, which prompts 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 PowerShell SDK cmdlets or PowerShell SDK automation scripts. See the following examples.

**Example activities**

**Import the Virtual Apps and Desktops service App-V package discovery module**

```bash
import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

**Loop through the App-V Package store directory and upload each package**

```bash
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**

```bash
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVManagementServer.domain.net
```
Citrix Virtual Apps and Desktops service

Discover Microsoft App-V Management and Publishing Servers and add the configuration to the Application Library

This also imports all the packages managed by the Microsoft App-V Management Server in dual admin mode.

```
```

Read PowerShell help documentation included in the module

```
1 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.
- The service management console in Citrix Cloud does not have a live connection to the Microsoft App-V Management server. Changes to Packages and other configuration in the Microsoft App-V Management server are not reflected in the service management console until `Import-AppVDualAdminCloud` is rerun. This is different to the on-premises package discovery behavior (described in the App-V documentation).

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

Citrix Virtual Apps and Desktops service APIs

The Virtual Apps and Desktops service APIs are available at https://developer.cloud.com/virtual-apps-and-desktops.

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 claims arising from your use, modification, or distribution of the code.

Copied!
Failed!