What's new

Cumulative Update 4 (CU4) is the latest release of the Citrix Provisioning™ 2402 LTSR. CU4 has one fix compared to the 2402 LTSR initial release, CU1, CU2 and CU3 of Citrix Provisioning.

What’s new in 2402 LTSR (initial release)

This release of Citrix Provisioning includes the enhancements described in the following sections. It includes several fixes for issues seen in past releases, and issues that we have identified.

Support for creating Citrix Provisioning catalogs using MCS PowerShell commands in VMware

You can now create Citrix Provisioning catalogs using MCS PowerShell commands in VMware.

This implementation provides you the following advantages:

- A single unified API to manage both MCS and Citrix Provisioning catalogs.
- Have new features for Citrix Provisioning catalogs, such as, identity management solution, on-demand provisioning, and so on.

For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

Update licenses to enable telemetry uploads

As outlined at Required License Server Update, Cloud Software Group has updated the license requirements that require you to upload telemetry. This implementation implies that as a Citrix Provisioning customer, you must return and allocate your Citrix Virtual Apps and Desktops and Citrix Provisioning license. For more information on licenses, see Licensing.

Support for installing Citrix Provisioning servers on Windows Server Core

With this feature, you can now install Citrix Provisioning servers on the system running Windows Server Core. The Server Core option is a minimal installation as opposed to the installation of Server with Desktop Experience. The Windows Server core reduces the potential attack surface to critical infrastructure.

The benefits of using this feature are:

- Enhanced security for the Citrix Provisioning Servers.
- Reduced cost because you can use a smaller VM.

The current limitations of this feature are:

- You cannot create target VMs using Citrix Virtual Apps and Desktops™ Setup Wizard using HDD BDM boot.
- You cannot do a BDM update using the Citrix Provisioning Console.

Support for XenServer® 8

With this feature, you can now use the Citrix Virtual Apps and Desktops Setup Wizard to create target VMs on a XenServer 8 host. For more information on XenServer 8, see About XenServer 8.

Support for new Linux streaming target devices

For Linux streaming, the following operating systems are now supported:

- SUSE 15.5

For more information, see Streaming Linux target devices.

Features supported from previous releases

The Citrix Provisioning 2402 LTSR supports all the features from Citrix Provisioning version 2206 CR and later. To list some of the key features:

You can see the following What's New articles to know about the features supported each in each CR:

- What’s New 2206
- What’s New 2209
- What's New 2212
- What's New 2303
- What's New 2305
- What's New 2308
- What's New 2311

Cumulative Update 4 (CU4)

Release date: May 08, 2026

What's new

Support for the New Microsoft SecureBoot CA Certificates

As documented by Microsoft at Windows Secure Boot certificate expiration and CA updates - Microsoft Support, the current certificates used for validating binaries when using Secure Boot are expiring in 2026 and have been replaced by new CA certificates which will be used in the future to validate that binaries are properly signed. This release of Citrix Provisioning includes support for secure boot when these new certificates are being used. See Windows Secure Boot certificate expiration and CA updates for details on how you can prepare for supporting secure boot once this has happened.

It is vital that you start the process of upgrading the hypervisor and existing VMs as well as upgrading to a version of Citrix Provisioning that supports the new certificates now to avoid outages starting in June 2026.

For more information, see Windows Secure Boot certificate expiration and CA updates.

About this release

Citrix Provisioning 2402 LTSR Cumulative Update 4 (CU4) fixes one issue reported since the initial release, CU1, CU2 and CU3 of the 2402 LTSR.

Citrix Provisioning (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 2402 LTSR CU4

Compared to: Citrix Provisioning™ 2402 LTSR CU3

Citrix Provisioning 2402 LTSR CU4 contains all fixes included in the 2402 LTSR initial release, CU1, CU2, CU3 plus the following, new fixes:

Citrix Provisioning target device issues

- When Daylight Saving Time (DST) changes and the vDisk was created with a different time value, target devices start with the incorrect time at boot due to mismatched registry settings.

Cumulative Update 3.1 (CU3.1)

Release date: August 27, 2025

What's new

File-based licensing system EOL notification

File-based licensing system, traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license Citrix on-premises components after April 15, 2026. To remain supported, your Citrix Provisioning deployment must be on a LAS compatible version. The minimum required Citrix Provisioning versions that are LAS compatible are:

- Citrix Provisioning 2203 LTSR CU7.1
- Citrix Provisioning 2402 LTSR CU3.1
- Citrix Provisioning 2507.1 LTSR

If you have questions or concerns, contact Customer Care. Citrix might limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix might have at law or equity. These requirements don't apply where prohibited by law or regulation.

Support for Citrix Cloud Licensing

PVS licensing has been updated to support the cloud license activation service. Customers currently using legacy licensing should see no change and will still be entitled to run PVS VDAs based on having either CVAD or PVS standalone license. However, two important changes have been made to the PVS Configuration Wizard run on every PVS server after installing/upgrading:

- You can no longer skip checking License Server connectivity.
- The License Server is required to be current - the CW will report an error if the version you have is too old.

The licensing tab on the configuration wizard has been updated to remove the license type (on-premise or cloud) as this is no longer required.

In addition, the license server connectivity is also checked when running the configuration wizard silently with an answer file. One new parameter is required in the answer file: the thumbprint of the LS certificate IF the license server is using a self-signed certificate (see Manually install a certificate used by the Citrix Licensing Manager and Web Services for Licensing). When running silently, if the check fails, then the CW fails. You can review the `C:\ProgramData\Citrix\Provisioning Services\Logs\Configwizard.log` file to find the error.

In a POC or small deployment, you can run the license server on one PVS Server machine so long as it is accessible from ALL PVS servers (see Firewall considerations for information on configuring firewalls to enable the license server).

Once you switch to using Cloud Licensing in the License Server, PVS will automatically use the status of your PVS Entitlement in the cloud service to control PVS licensing. If you have no PVS entitlement, it will fall back to checking for legacy licenses.

About this release

Citrix Provisioning 2402 LTSR Cumulative Update 3.1 (CU3.1) fixes six issues reported since the initial release, CU1 and CU2 of the 2402 LTSR.

Citrix Provisioning (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 2402 LTSR CU3.1

Compared to: Citrix Provisioning™ 2402 LTSR CU2

Citrix Provisioning 2402 LTSR CU3.1 contains all fixes included in the 2402 LTSR initial release, CU1, CU2 plus the following, new fixes:

Citrix Provisioning server issues

- Linux target might lose it's Active Directory trust and is not be able to access domain resources.
- You might experience an issue where the system throws an error every 5 minutes during data uploads and also at startup.

- You might experience server failure to respond to a request in time, which could cause the system to treat all registry values as plaintext.
- The Citrix Virtual Desktops™ Setup Wizard and Streamed VM Setup Wizard might fail to import existing computer accounts without Create Computer objects and Delete Computer objects permissions for the organizational unit. You get the error: Unable to move the Active Directory account to the requested Organizational Unit, although the Active Directory account movement is not the actual issue. Similarly, resetting a machine account password without specifying a new organizational unit can fail due to the same permission requirements.

Citrix Provisioning target device issues

- When creating Citrix Provisioning targets using Studio, domain trust is sometimes lost leading to a failure to register the VDA with the broker.
- You might be unable to launch a session and experience issues with policies being applied after upgrading to 2402 LTSR CU2.

Citrix Provisioning license issues

- Citrix Provisioning becomes unlicensed after 24 hours when using legacy license files.
- Citrix Provisioning didn't support perpetual legacy licenses.
- Citrix Provisioning didn't check the Software Assurance (SA) date included within legacy license files. License validation logic has been updated to strictly enforce the SA date. Citrix Provisioning now requires the SA date on the installed license to be current (equal to or newer than) the build date of the Citrix Provisioning release being used.

Cumulative Update 2 (CU2)

Release date: March 07, 2025

What’s new

Support for Windows Server 2025 and Windows Server Core 2025

Citrix Provisioning™ 2402 LTSR CU2 now supports Windows Server 2025 and Windows Server Core 2025.

Telemetry data elements

With respect to the usage telemetry reporting, following additional data elements are added to process data on how licenses are utilised.

- Count of Citrix Provisioning Farms
- Count of Citrix Provisioning Sites
- Count of Citrix Provisioning Servers
- Count of Citrix Provisioning vDisks that exist (not a count of those that are in use)

Create Citrix Provisioning catalogs using MCS PowerShell commands in XenServer®

You can now create Citrix Provisioning catalogs using MCS PowerShell commands in XenServer environments. You can create both machine-profile based and non-machine profile based Citrix Provisioning catalogs. For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

About this release

Citrix Provisioning 2402 LTSR Cumulative Update 2 (CU2) fixes nine issues reported since the initial release and CU1 of the 2402 LTSR.

Citrix Provisioning (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 2402 LTSR CU2

Compared to: Citrix Provisioning™ 2402 LTSR CU1

Citrix Provisioning 2402 LTSR CU2 contains all fixes included in the 2402 LTSR initial release, CU1 plus the following, new fixes:

Citrix Provisioning console issues

- In Citrix Provisioning 2402, you cannot copy properties (VDisk assignments) from one target device to another after upgrading from PVS 2311.

Citrix Provisioning server issues

- After upgrading Provisioning Services (PVS) Servers from version 1912 CU3 to 2402, target devices may fail to boot due to a TFTP error if the PVS Server has multiple network connections and TFTP is set to use the management network connection.

- You may sometimes see a blank cache volume drive letter in Windows Management Instrumentation (WMI) `root\Citrix\PVS_Target class`.
- The problem reporting causes 100% CPU usage in the database and the problem report status is stuck as Initiated on all Citrix Provisioning Servers.
- Silent upgrade of Citrix Provisioning components sometimes generated popups. This is fixed if you upgrade from 2203 CU4 to 2203 CU6 or later, or, 2203 CU6 or later to 2503 or later.
- If the Citrix Provisioning target device is installed when running as the system account, the installation is successful, but the package is not shown in "add/remove programs"
- Citrix Provisioning vDisk WMI sometimes returns blank result for cache volume drive letter.
- When you use Citrix Provisioning Boot Device Manager (BDM.exe) to create a new Unified Extensible Firmware Interface (UEFI) boot entry, the bootable UEFI disk might not be created correctly if the device is a non-Operating System (OS) disk.

Citrix Provisioning target device issues

- When you use Citrix Provisioning Boot Device Manager (BDM.exe) to create a new Unified Extensible Firmware Interface (UEFI) boot entry, the bootable UEFI disk may not be created correctly if the device is a non-Operating System (OS) disk.

Cumulative Update 1 (CU1)

Release date: October 16, 2024

What’s new

Enhancement to the usage telemetry reporting

The usage telemetry reporting feature is now enhanced to collect and process data on how licenses are utilised for Citrix® products, components, and features that are deployed in customer-managed environments. This enhancement ensures compliance with licensing for Citrix on-premises products.

To leverage this enhancement, update to the latest version of the license server. For more information, see:

- Citrix licensing telemetry
- Required license server updates
- Citrix license telemetry faq

For the list of Citrix Provisioning telemetry data elements, see Citrix Provisioning telemetry data elements.

In Citrix Provisioning™, the connection to the license server is tested after you click **Next** on the **License Server** page of the Configuration Wizard.

For the changes related to the Configuration Wizard and farm properties, see:

- Configuration wizard: Select the license server
- Farm: licensing tab
- Running the configuration wizard silently

Support for enabling Citrix Provisioning Accelerator for targets using IPv6 streaming

With this feature, when using XenServer8, you can enable Citrix Provisioning Accelerator for targets using IPv6 streaming. For more information, see Citrix Provisioning Accelerator.

About this release

Citrix Provisioning 2402 LTSR Cumulative Update 1 (CU1) fixes five issues reported since the initial release of the 2402 LTSR. It also includes support for Microsoft SQL Server 2019.

Citrix Provisioning (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 2402 LTSR CU1

Compared to: Citrix Provisioning™ 2402 LTSR initial release

Citrix Provisioning 2402 LTSR CU1 contains all fixes included in the 2402 LTSR initial release, plus the following, new fixes:

Citrix Provisioning console issues

- Citrix Provisioning auditing does not track shutdowns you initiate from the Provisioning Console. When you enable the audit trail, it will not log your successful or unsuccessful shutdown attempts from the console.

- In Citrix Provisioning, some user accounts from a different domain cannot access the Provisioning Console due to issues accessing the domain's Active Directory.
- In Citrix Provisioning 2402, you cannot copy properties (VDisk assignments) from one target device to another after upgrading from PVS 2311.

Citrix Provisioning server issues

- Upgrading from earlier PVS releases to 2402-GA would sometimes lead to failures in upgrading the database schema in the configuration wizard - these issues are addressed in the 2402-CU1 release.

Citrix Provisioning target device issues

- You might experience intermittent file corruption, especially during the login process when user profiles are downloaded and written to the PVS drive. This issue affects various file types and occurs on PVS target devices running Windows Server 2022.

What's new

This release of Citrix Provisioning includes the enhancements described in the following sections. It includes several fixes for issues seen in past releases, and new issues that we've identified.

Support for SCVMM 2025

Citrix Provisioning now supports Microsoft's System Center Virtual Machine Manager (SCVMM) 2025. For more information about the new features supported in SCVMM 2025, see What's new in System Center Virtual Machine Manager.

Support for Windows Server 2016 in Citrix Provisioning™ on Azure

Citrix Provisioning now supports Windows Server 2016 on Azure.

Support for Windows 11 in Citrix Provisioning on Azure

Citrix Provisioning now supports Windows 11 on Azure **Standard** security type. Security type refers to the different security features available for a virtual machine. You can select the security type when you create a VM on Azure console.

Configuration wizard changes for database credentials

The Configuration wizard now always prompts for database administrator credentials, and uses those credentials to configure the provisioning database. You can now select **Active Directory**

Integrated authentication when providing database administrator credentials, which accesses the provisioning database as the current logged in user.

Azure Marketplace

Citrix Provisioning does not support Azure Marketplace images with plan information. For more information, see Citrix Provisioning on Microsoft Azure.

Support for both Customer Managed and Citrix Cloud™ Delivery Controllers natively from the same Citrix Provisioning Console

Citrix Provisioning now supports working with both customer managed and Citrix Cloud Delivery Controllers natively from the same Citrix Provisioning Console. It no longer uses the five PowerShell snap-ins for communicating with on-premises Delivery Controller. There is also no need to manually uninstall or reinstall PowerShell modules to switch between on-premises and cloud Delivery Controllers.

While running the Citrix Virtual Desktops™ Setup and Citrix Provisioning Devices Export Wizard, you can now select either **Citrix Cloud** or **Customer-Managed Control Plane** Delivery Controller.

Support for Device Guard on ESX 6.7 or newer, and ESX 7.0 update 3

Citrix Provisioning now supports the following enabled with Device Guard using ESX 6.7 and above, and ESX 7.0 update 3:

- Targets running on Windows 10, Windows 2016, or Windows 2019.
- Citrix Provisioning server on Windows Server 2016, Windows Server 2019, or Windows Server 2022.

For more information, see Deployments using Device Guard.

Support for Hybrid Rights License

Citrix Provisioning now allows use of Hybrid Rights License with Citrix licensing server. For more information, see the following:

- Transition and Trade-Up (TTU) with Hybrid Rights
- Upgrade a deployment
- Citrix Provisioning-Licensing
- System Requirements

Fixed issues

Citrix Provisioning™ 2402 LTSR includes the following fixed issues:

- After you upgrade to Citrix Provisioning 2311, the Citrix Provisioning Console doesn't provide the option Farm is already configured.
- You get an unexpected MAPI error when you click Search on the Add or Import Existing vDisks dialog to display all the vDisks in the store.
- While using the Citrix Virtual Apps and Desktops™ Setup Wizard in the Azure environment to create VMs using a template, the tags of the template do not match the tags of the created VMs.
- In Citrix Provisioning version 2311 and earlier, IPv6 in Citrix Provisioning streamed Windows targets that use IPv4 streaming is not supported.
- When your farm is joined to a Citrix Virtual Apps™ and Desktops site, the Configuration Wizard might not properly validate that the user has sufficient privileges on the Delivery Controller that is selected. You might get the privilege errors only during the finish step. Therefore, always ensure that you have Machine Catalog Administrator or higher privileges in the Citrix Virtual Apps and Desktops site.
- Upgrade from Citrix Provisioning version 2308 to Citrix Provisioning version 2311 is not supported on Azure. If you try to upgrade, the Citrix Provisioning console and server are left in a broken state that can only be cleaned up using a tool like **MSIZap**. However, upgrading from any version to 2402 LTSR works.
- While running the Configuration Wizard to create a new farm, if you provide database administrator credentials that do not have `dbcreator` privileges, you are repeatedly prompted to provide different credentials without any message explaining the reason. To exit this condition, provide the required credentials or click **Cancel** on the **Database Administrator Credentials** dialog.
- When running a BDM update in the Citrix Provisioning Console, an incorrect message **The task cannot be performed on active Devices. Shut down the Devices before attempting to perform the task** is displayed when the hypervisor is not accessible.
- Windows 2022 as a host has limitations. Microsoft SCVMM 2019 for Hyper-V does not support Windows Server 2022 as a host. The Citrix Virtual Apps and Desktops Setup wizards and Stream VM wizard cannot create targets when using Windows Server 2022 as the hypervisor.

Known issues and considerations

Known issues in 2402 LTSR CU1

- P2PVS cannot create a vDisk when the VM being imaged is booted with UEFI. As a workaround, use Imaging Wizard. For example, run `c:\\Program Files\\Citrix\\Provisioning Services\\ImagingWizard.exe P2vhdx win10 c:\\test` to create a VHDX file named `win10` in `c:\\test` .

  When you use UEFI imaging, consider the following:

  - You cannot specify individual volumes. UEFI imaging operates on the entire boot disk.
  - UEFI imaging does not support multiple disks. The system images only a single boot disk configuration.

- When upgrading from PVS 2203 CU6 to PVS 2303 (or any version before 2402 CU1), if the Farm is opted to join to Cloud, the Farm's Encryption Key rotation state might remain in **Distributing Keys** state and not move to the next state. To resolve this issue:

  a. To move the Encryption's Key Rotation state to **Re-Encrypting database**.

  b. Manually navigate to the **SQL Server -> -> ScheduledWork table**.

  c. Manually delete the rows that have the `jobName = "UsageTelemetry"` and `FarmMetrics`.

  d. Wait for 5 mins and then check the **Encryption** Tab in **Farm** Properties in the Citrix Provisioning™ Console.

Known issues in 2402 LTSR

This Citrix Provisioning release includes the following new issues and considerations:

- If you upgrade from a system that was created before 7.12 to 2402 LTSR initial release, the upgrade fails while running the Configuration Wizard with a database upgrade error.

  The upgrade doesn't fail if you try to upgrade to a version earlier than Citrix Provisioning 2402 LTSR initial release.

- If an admin is a member of multiple groups configured as Citrix Provisioning admins, then if any group is made Read-only, then all admins in that group become Read-only admins even if they are members of other groups that are not set to Read-only.
- If you are on Citrix Provisioning version 1912 LTSR CU9 or earlier, 2203 LTSR CU5 or earlier, or 2402 LTSR or earlier CRs, and upgrade your license from DaaS to Universal Hybrid Multi Cloud License (UHMC) or Platform License (CPL), then you receive an on-premises universal license file which contains `PVS_CCS` and `PVSD_CCS` licenses. To configure your new licenses, run the Configuration Wizard to change the license type from **Cloud** to **On-premises** on the **License Server** page.
- Citrix Provisioning does not currently support IPv6 on Nutanix. However, while running the Citrix Virtual Desktops™ Setup Wizard to create VMs on Nutanix, you incorrectly get the option to select **Targets use IPv6** checkbox on the **Virtual machines** page. .

Previously reported issues

- The help text displayed using `Get-Help -examples New-BootDeviceManager` does not include information on the new parameters added to support IPv6 addresses.
- If you want to create VMware target VMs, that stream using IPV6, from a template that was created from a VM that was run previously, then all the target VMs get the same DHCP Unique Identifier (DUID) value. To resolve the issue, use a template that's created from a VM that was never run before. This action ensures that the VMware target VMs get a unique DUID value each time the target VMs are run.
- The Citrix Virtual Apps and Desktops™ Setup Wizard sometimes fails to provision targets on Nutanix if the **Auto-Add** feature is enabled on the Citrix Provisioning console.
- In GCP environments, the Citrix Virtual Apps™ and Desktops Setup Wizard fails to remove server-side write cache files that are in the `WriteCache` directory of the Citrix Provisioning store. The write cache files are used to format the write cache when you first start the VMs. Therefore, the files must be removed even if provisioning fails to avoid wasting disk space. To resolve this issue, do one or both of the following:
  - Ensure that the number of threads has a value of 20. Do one of the following:
    - Set the value in the registry setting key:

```
Computer\HKEY_CURRENT_USER\Software\Citrix\ProvisioningServices\VdiWizard\MAX_VM_CREATE_THREADS_PER_HYPERVISOR
```

    - Remove the registry setting key.
  - Ensure that the store used for write-cache files uses an **SSD persistent disk** instead of a **Standard disk**.

- The Stream and SOAP services crash and do not start after installing Microsoft January 2022 updates. To resolve the issue, check the event log in the **Event Viewer > Application**. If the log mentions about forest trust relationship information, do one of the followings:
  - Apply the Microsoft fix based on your OS, Citrix Provisioning version, and version of the `.NET` framework. For more information, see CTX338544.
  - Set a DWORD registry value named `SkipForestLevelTrusts` to `1` under `HKLM\Software\Citrix\ProvisioningServices` on the Citrix Provisioning Server and restart the SOAP Server. With this workaround, Citrix Provisioning stops supporting multiple forest deployments.

- If you use IPv6-based streaming, then the streamed target acquires two IPv6 addresses from DHCP, out of which, one of the addresses shows up as a statically assigned address in Windows. You can also see an auto-configured address if IPv6 auto-configuration is enabled on the network. This auto-configured address also shows up as a statically assigned address in Windows. In addition to these, the streamed target is also allocated a link local address in Windows.
- In Citrix Provisioning on Azure 2112 and later, some of the VMs fail to release vDisk lock even after shutting down the VMs.
- When configuring boot devices using the **Boot Device Management utility**, you cannot proceed beyond the **Specify the Login Server** page if you:

  a. Select **Use DNS to find the server**.
  b. Select the **Target Device is UEFI firmware** checkbox.
  c. Enter an FQDN longer than 15 characters in the **Server FQDN** field.
  d. Clear the **Target Device is UEFI firmware** checkbox.
  e. Select **Use static IP address for the Server**.

  You can continue to the next page if you clear the FQDN field or reduce the number of characters to fewer than 15.
- The Citrix Virtual Desktops Setup Wizard creates targets then boots them to format the cache drive. This process occurs quickly. Sometimes, a VDA reaches a state where it fails to shut down correctly. This process occurs because the VDA is initializing while the Citrix Provisioning

Service and the provisioned device service simultaneously finish formatting the cache drive, then shuts down. To resolve this issue:

a. In the virtual disk registry key, `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices`, create a DWORD called `RebootDelaySec`.

b. Assign a value to `RebootDelaySec`. This delays the time for shutdown by the value set in seconds.

- When using the Streamed VM Setup Wizard to create VMs on a XenServer host while specifying 1 vCPU, the VM is created with 1 vCPU and a topology of 2 cores per socket. Creating VMs in this fashion prevents the VM from booting, while displaying the following error message in XenCenter®: “The value ‘VCPU_max must be a multiple of this field’ is invalid for field platforms: cores-per-socket. As a result, XenCenter fails to boot the VM because the topology and vCPU configuration are incompatible.

Data governance

Citrix Provisioning™ collects and transmits data to Citrix in the following cases:

- When provisioning target VMs, information about those VMs is transmitted to Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service).
- When problem reports are generated with the Citrix Provisioning Console, a set of data is collected from the Citrix Provisioning servers and saved as a diagnostic bundle. Citrix customer support provides instructions on making the diagnostic bundle available to them.

The following sections detail the data items included in these two use cases.

Provisioning data

The following data is transmitted to Citrix DaaS™:

- VM names representing target VMs that are added to Citrix Virtual Apps™ and Desktops broker catalogs.
- In addition, the Active Directory computer account SIDs for those target VMs is supplied. These are unique identifiers for the Active Directory computer accounts in the customers Active Dirtectory Domain.

Support bundle data

The support bundle generated by Citrix Provisioning consists of a ZIP file with the following files. These files contain customer data for each targeted Citrix Provisioning Server:

FILE	CONTENT
header.json & server-name.json	Citrix Provisioning Server hostname, local and domain SID, machine UUID, OS version, summary of problem, Citrix Provisioning farm ID
journal.json	Log of problem report generation

FILE	CONTENT
Manifest.xml	The username that the Citrix Provisioning service is running as.
process.json	List of running processes on the Citrix Provisioning Server.
registry.json	Complete dump of `HKLM\SOFTWARE\Citrix` registry tree. Includes encrypted data covering the database connection.
AOTraces/*.etl	Windows ETL files containing Citrix Provisioning service logs. These are sanitized and contain no sensitive data.
Event Logs/*.csv	Windows application and system event logs from the Citrix Provisioning Server.
Hardware/*	Hardware details including details of all hardware, network connection details (including IP address and MAC address of Citrix Provisioning server), logical drives, pagefile usage.
Registry/*	Dump of `HKLM\Software\Citrix, HKLM\Software\Microsoft\Cryptography, HKLM\CtrlPanel\Desktop, HKLM\Software\Microsoft\Windows\CurrentVersion\Policies, HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon, HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows, HKLM\Software\Wow6432Node\Citrix, HKLM\Software\Wow6432Node\Microsoft\Cryptography, HJKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer, HKLM\System\CurrentControlSet\Control\Citrix, HKLM\SYSTEM\CurrentControlSet\Control\`

FILE	CONTENT
	`FileSystem, HJLM\SYSTEM\CurrentControlSet\Control\SystemInformation, HJKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation, HKLM\System\CurrentControlSet\Control\Terminal Server, HKLM\SYSTEM\CurrentControlSet\Control\Windows, HKLM\SYSTEM\CurrentControlSet\Control\Print\Environments, HKLM\System\CurrentControlSet\Control\Session Manager`
Software/*	Files containing the software environment including: list of installed drivers, environment variables for user running Citrix Provisioning, output of `GPResult` command, list of installed Microsoft Hotfixes, output of netstat command showing listening and running TCP and UDP ports, OS Version, list of Windows Services.
pvs.zip	See below.

The `pvs.zip` file contains:

FILE	CONTENT
PVSLogs\ConfigWizard.ans	Contains all of the answers provided when running the configuration wizard including the username and encrypted password for the user running Citrix Provisioning, and log files generated when the wizard runs.
PVSDatabase*,xml	Sanitized dump of Citrix Provisioning database. All sensitive data including usernames and passwords is removed from this data.

Third-party notices

The current release of Citrix Provisioning™ might include third-party software licensed under the terms defined in the following document:

Citrix Provisioning 2402 third party notices (PDF Download)

Deprecation

The announcements in this article are intended to give you advanced notice of features which are being phased out so that you can make timely business decisions. Citrix® monitors customer use and feedback to determine when they are withdrawn. This list is subject to change in subsequent releases and does not include every deprecated feature or functionality.

The following features are *deprecated*. This does not mean that they are removed immediately. Citrix will continue to support them up to and including the next Citrix Provisioning version that is part of the next Citrix Virtual Apps and Desktops™ Long Term Service Release (LTSR). Deprecated items will be removed in a Current Release following the next LTSR. Alternatives for deprecated items are suggested where possible.

For complete details about product lifecycle support, see the Product Lifecycle Support Policy article.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	ALTERNATIVE
Support for BOOTP service. You can only use this service for BIOS	2402 LTSR	Configure UEFI PXE boot. See Unified Extensible Firmware Interface (UEFI) pre-boot environments.
Support `.vhd` format for vDisk	2402 LTSR	Use `.vhdx` format.
Support for Streamed VM Setup Wizard	2402 LTSR	Use Citrix Virtual Apps™ and Desktops Setup Wizard for VDAs.
Support for Subnet affinity	2402 LTSR	None
Support for Upgrade Wizard	2402 LTSR	None
Support for Accelerated Office Activation	2402 LTSR	Configure GPO policies. For more information, see Work with policies.

ITEM	DEPRECATION ANNOUNCED IN RELEASE	ALTERNATIVE
Support for BIOS in Citrix Provisioning	This platform is deprecated from version 2203. In version 2311, targets configured to boot using BIOS continues to function. However, BIOS management dialogs have been removed from 2311 release	You must migrate to using UEFI booting. All new features, such as IPv6 will be UEFI in the future. For information on converting BIOS vDisks to UEFI, see Converting BIOS vDisks to UEFI.

System requirements and compatibility

The system requirements in this article were valid when this Citrix Provisioning™ version was released. Updates are made periodically. Components not covered here (such as StoreFront, host systems, and Citrix Receivers) are described in their respective documentation.

For more information about using this Current Release (CR) in a Long Term Service (LTSR) environment and other FAQ, see the Knowledge Center article.

> **Important:**
>
> Review the preinstallation tasks article before installing Citrix Provisioning.
>
> Unless otherwise noted, the component installer deploys software prerequisites automatically (such as .NET elements) if the required versions are not detected on the machine. The Citrix® installation media also contains some of this prerequisite software.

For internationalization information, see Global Status of Citrix Products.

Database

For the list of supported databases, see Citrix Virtual Apps and Desktops- System requirements.

Citrix Provisioning supports SQL Server 2022 in the following on-premises configuration:

- Standalone
- Database mirroring
- Always on failover with or without multi-subnet failover

For information about database support for Citrix Provisioning on Microsoft Azure, see Azure database services.

SQL Server Native Client support is removed from Citrix Provisioning 2109 and later. Microsoft OLE DB Driver is now installed with specific Citrix Provisioning versions. Citrix Provisioning 2308

and later supports Microsoft OLE DB Driver 19.3 or later to meet security compliance and performance requirement.

> **Note:**
>
> Currently, Citrix Provisioning does not support installing the SQL Server in the Operating System where the Citrix Provisioning Server is installed. However, this scenario is possible in the testing environment.
>
> Database clustering is supported.

When configuring databases for provisioning, consider that no preference exists for any specific SQL collation. Collation supports the standard method recommended by Citrix Virtual Apps and Desktops when using the configuration wizard. The administrator creates the database with a collation that ends with `_CI_AS_KS`. Citrix recommends using a collation that ends with `_100_CI_AS_KS`. Collation requirements differ for earlier Citrix Provisioning releases. See FAQ: Recommended database collations for Citrix Products for more information.

> **Note**
>
> See Supported Databases for Citrix Virtual Apps and Desktops Components in the Knowledge Center for additional information about supported databases and clients.

License

The Citrix Licensing Server download for this release is included with the Citrix Virtual Apps and Desktops™ installation media. Use the most recent Citrix License Server to get the latest features.

> **Important:**
>
> Citrix Provisioning servers must be connected to the License Server to operate successfully. Use the most recent version of the Citrix License Server to get the latest features. Citrix recommends that you upgrade the License Server **before** upgrading Citrix Provisioning to avoid any licensing conflicts related to grace periods. For more information, see Licensing.

Provisioning server

Operating systems

- Windows Server 2025
- Windows Server Core 2025

> **Note:**
>
> Windows Server 2025 and Windows Server Core 2025 are supported on Citrix Provisioning 2402 LTSR CU2 and later CUs, and 2407 and later.

- Windows Server 2022
- Windows Server Core 2022
- Windows Server 2019
- Windows Server 2016

> **Note:**
>
> The current limitations of installing Citrix Provisioning servers on the system running Windows Server Core are:
>
> - You cannot create target VMs using Citrix Virtual Apps™ and Desktops Setup Wizard using HDD BDM boot.
> - You cannot do a BDM update using the Citrix Provisioning Console.

Refer to the Citrix Virtual Apps and Desktops System Requirements page for a complete list of supported provisioning server operating systems.

English, Japanese, and Simplified Chinese versions are supported.

Processors

The following processors are supported:

- Intel or AMD x64 compatible; 2 GHz minimum; 3 GHz preferred

- 3.5 GHz Dual Core/HT or similar for loads greater than 250 target devices
- A Citrix Provisioning server with 2 vCPUs.

Memory sizing

The recommended memory sizing for the Citrix Provisioning Server is:

2GiB + (Multi-Session-OS_vDisk x 4GiB) + (Single-Session-OS_vDisk x 2GiB) + 15% (Buffer)

Storage

A Provisioning Server can have many vDisks stored on it, and each disk can be several GB in size. Improve your streaming performance by using a RAID array, SAN, or NAS.

There must be enough space on the hard disk to store the vDisks. For example, if you have a 15 GB hard drive, you can only create a 14 GB virtual disk.

More requirements depend on several factors such as:

- **Hard disk capacity** – The requirements of the operating system and applications running on a target device. Citrix recommends adding 20% to the base size of the final installed image.
- **Private Image Mode** – The number of target devices using a virtual disk in private image mode. vDisks in private image mode are backed up daily.
- **Standard Image Mode** – The number of target devices using a virtual disk in standard image mode. Best practice is to include making a copy of every virtual disk created. Minimum estimated common storage sizes:
  - 250 MB for the database
  - 5 GB on a clean Windows system
  - 15 GB per virtual disk for Vista Class images

Network adaptor

- Static IP, 1 network connection with Gb Ethernet, or higher preferred
- Dual 1 GB Ethernet for more than 250 target devices
- Two NICs often perform better than a single dual-ported NIC

> **Note:**

> For information specific to network adapters for Citrix Provisioning on Microsoft Azure, see Citrix Provisioning on Microsoft Azure.

Citrix Provisioning dependencies

The Citrix Provisioning server installs program requires Microsoft NET 4.8 and Windows PowerShell 4.0.

Network

> **Note:**

> During normal operations, Citrix Provisioning Servers communicate with other Citrix Provisioning Servers, even across sites. Therefore, the network must support any-to-any connectivity between all Citrix Provisioning Servers, regardless of their site location.

> The following list describes each network type and the associated port.

UDP and TCP ports

- **Provisioning server to provisioning server communication:** Each provisioning server must be configured to use the same ports (UDP) to communicate with each other. At least five ports must exist in the selected port range. Configure the port range on the **Stream Services** dialog when running the Configuration Wizard.

  > **Note:**

  > If you are configuring for high availability, all provisioning servers selected as failover servers must reside within the same site. High availability is not intended to cross between sites.

  > **Default port range (UDP):** 6890–6909

- **Provisioning servers to target device communication:** Each provisioning server must be configured to use the same ports (UDP) to communicate with target devices using the

StreamProcess. The port range is configured using the **Console Network** tab on the **Server Properties** dialog.

> **Note:**
>
> The first 3 ports are reserved for Citrix Provisioning.
>
> **Default port range (UDP):** 6910–6930

- **Target device to Citrix Provisioning communication:** Unlike provisioning servers to target device port numbers, which you can configure using the configuration wizard, target device to Citrix Provisioning communication cannot be configured because the client port numbers are static.

> **Tip:**
>
> Make sure that port 6901 is open for target device communication. If you are using the installation wizard to open ports manually, be sure to include port 6901 to prevent communication problems between the target device and provisioning server. If you have chosen to use the default settings when using the wizard, you will not have the option to manually set this port.
>
> **Ports (UDP):** 6901, 6902, 6905

- **Login server communication:** Each provisioning server used as a login server must be configured on the **Stream Servers Boot List** dialog when running the Configuration wizard.

  Default port (UDP): 6910

- **Citrix Provisioning console communication:** The SOAP Server is used when accessing the provisioning console. The ports (TCP) are configured on the **Stream Services** dialog when running the Configuration Wizard. For PowerShell: `MCLI-Run SetupConnection`. For MCLI: `MCLI Run SetupConnection`.

Trivial FTP (TFTP)

- The TFTP port value is stored in the registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BNTFTP\Parameters Port

Default port (TFTP): 69

TSB

- The TSB port value is stored in the registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PVSTSB\Parameters Port

  Default port (UDP): 6969

  Port Fast: Port Fast must be enabled

  Network card: PXE 0.99j, PXE 2.1 or later

  Addressing: DHCP

> **Note:**
>
> **Citrix Provisioning console to Provisioning server communication:** While using Citrix Provisioning console to specify a Citrix Provisioning server, use a hostname instead of a numeric IP address. This implementation ensures that the insecure Windows NT LAN Manager (NTLM) protocol is not used and might be disabled on your network. If you want to use a numeric IP address, then you must configure the DNS reverse lookup zones to translate the IP address to a hostname.

Supported IP addresses

Citrix Provisioning supports the following types of streaming IP addresses:

- IPv4
- IPv6

> **Note:**
>
> Citrix Provisioning supports streaming of only UEFI based targets over IPv6. This feature is applicable to the following hypervisors:
>
> - VMware 7.x

- VMware 8.x
- Hyper-V
- Azure
- XenServer® 8

Requirements to stream targets over IPv6 are:

- Enable DHCv6: the DHCPv6 Server must include the DNS Servers option (option 23) if you want to use DNS names to locate the server to connect to.
- Routers must publish the prefix route for the IPv6 network.

Target device

In most implementations, there is a single virtual disk providing a standard image for multiple target devices. To simplify virtual disk and target device maintenance, create and maintain fewer vDisks and assign more target devices to each virtual disk.

Tip:

When using the virtual disk Imaging Wizard for a target device, problems appear related to some Microsoft components which are not installed. For example, operating systems that do not have Microsoft Visual C++ generate an error message similar to:

```
api-ms-win-crt-runtime-11-1-01.dll is missing
```

Citrix recommends that all Windows updates and components are current before installing Citrix Provisioning.

When provisioning target devices, consider the following:

- To have a single virtual disk, all target devices must have certain similarities to ensure that the OS has the necessary drivers required to run properly. The three key components are the motherboard, network card, or video card.

- Install and configure the OEM NIC teaming software before you install the target device software.
- Identify target devices by the operating system running on the device.
- Dual boot virtual disk images are not supported.
- BitLocker encryption is not supported on a provisioned target device virtual disk.
- Citrix Provisioning supports layered images for Citrix App Layering functionality. See the System requirements for more information.

Supported Operating Systems

- Windows Server 2025
- Windows Server Core 2025
- Windows Server 2022
- Windows Server Core 2022

> **Note:**
>
> The current limitations of installing Citrix Provisioning servers on the system running Windows Server Core are:
>
> - You cannot create target VMs using Citrix Virtual Apps and Desktops Setup Wizard using HDD BDM boot.
> - You cannot do a BDM update using the Citrix Provisioning Console.

- Windows Server 2019
- Windows Server 2016

> **Note:**
>
> Windows Server 2016 is not supported in target devices provisioned on Azure.

- All Microsoft supported Windows 11 versions
- All Microsoft supported Windows 10 versions

Refer to the Citrix Virtual Apps and Desktops System Requirements page for a complete list of supported target device operating systems.

Consider the following when provisioning target devices:

- Citrix Provisioning supports publicly available Windows OS version at the time of the release.
- Citrix recommends that you reboot after installing each Windows update.

Windows 10 limitations

For target devices running supported versions of Windows 10, note the following:

- Windows 10 v1803 target devices with virtual disk cache type set to **Cache in device RAM** possibly crash when booting.
- Citrix Provisioning supports Windows 10 Fall Creator v1709, however, a target device with this OS cannot boot from a virtual disk in private image mode.
- Windows 10 v1809 (x86 and x64) creates a page file error. For Windows 10 1803, this issue does not exist between versions 17134.0–17134.523. However, the issue appears when using Windows 10 1803 version 17134.556. See the Microsoft site for more information. For Windows 10 1809, this issue appears between versions 17763.0–17763.253. The issue is resolved in Windows 10 1809 version 17763.292. See the Microsoft site for more information.

> **Note:**
>
> Citrix Provisioning does not support Windows 10 IoT Core and Windows 10 IoT Enterprise. See the Microsoft site for more information.

About Gen 2 VMs

Gen 2 VMs are supported across all operating systems where Microsoft supports UEFI.

> **Note:**
>
> The Streamed VM wizard setup does not support SCVMM Gen 2 VMs\templates.

Linux streaming

Using the Linux streaming feature with Citrix Provisioning, you can provision Linux virtual desktops in the Citrix Virtual Apps and Desktops environment. For more information about the Linux streaming feature, see Use Citrix Provisioning to create Linux VMs

The following operating systems are supported for Linux streaming.

- Ubuntu 22.04, 20.04
- Red Hat Enterprise Linux 9.2, 9.0, 8.8, 8.6, 7.9
- Rocky Linux 9.2, 9.0, 8.8, 8.6
- SUSE Linux Enterprise Server 15 SP5

Be sure to follow the installation recommendations in Streaming Linux target devices.

More dependencies

.NET 4.8 (default)

Microsoft licensing

Consider the following when using Microsoft licensing keys with target devices:

- Windows 10, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2022 are deployed using either the Key Management Server (KMS) or with Microsoft Multiple Activation Key (MAK) volume licensing keys.
- Windows Office 2010, Office 2013, and Office 2016 are deployed using KMS licensing. Volume licensing is configured within the virtual disk image when the Imaging Wizard is run on the main target device. Volume licensing is configured for the virtual disk file on the Microsoft Volume Licensing tab, which is available from the **Console vDisk File Properties** dialog.

> **Note:**
>
> For MAK licensing to work, the Volume Activation Management Tool (VAMT) for that client OS must be installed on all login servers within a farm. In addition, both Private and Standard Image Modes support MAK and KMS.

File system type

- NTFS

- For Linux streaming, the following file system types are supported: EXT4, BTRFS, XFS.

Supported operating systems include English on English, Japanese, German, French, Spanish, Simplified Chinese, Traditional Chinese, Korean, and Russian versions.

Citrix Provisioning console

Processor: Minimum 1 GHz, 2 GHz preferred

Memory: Minimum 1 GB, 2 GB preferred

Hard disk: Minimum 500 MB

Operating systems:

- Windows Server 2025
- Windows Server Core 2025
- Windows Server 2022
- Windows Server Core 2022
- Windows Server 2019
- Windows Server 2016
- All Microsoft supported Windows 11 versions
- All Microsoft supported Windows 10 versions

> **Note:**

> Gen 1 VMs are not supported on SCVMM for Hyper-V with Windows Server 2022.

> **More dependencies:**

- MMC 3.0
- Microsoft .NET 4.8
- Windows PowerShell 3.0

Store

Ensure that the store can communicate with the Citrix Provisioning database.

Citrix Virtual Apps and Desktops Setup wizard

The Citrix Virtual Apps and Desktops Setup wizard can only operate with the equivalent version of the Citrix Virtual Apps and Desktops controller:

- One or more configured Citrix Virtual Apps and Desktops hosts with identical templates must exist.
- The virtual disk assigned to each VM must be in standard image mode.

More requirements include:

Permissions:

> **Tip:**
>
> Some of the permissions that are noted in this section relate only to on-premises deployments.
>
> Consider the following:

- A Citrix Virtual Apps and Desktops controller must exist with permissions for the current user.
- vCenter, Nutanix, SCVMM, and XenServer minimum permissions must be configured.
- A user accessing the Citrix Provisioning console must be configured as a Citrix Virtual Apps and Desktops administrator. The administrator must also exist in the provisioning **SiteAdmin** group.
- If you are using Citrix Provisioning with Citrix Virtual Apps and Desktops, the SOAP Server user account must have Citrix Virtual Apps and Desktops full administrator privileges.
- When creating accounts in the Console, the user needs the Active Directory Create Accounts permission. To use existing accounts, Active Directory accounts have to exist in a known OU for selection.
- When creating a machine catalog in Citrix Virtual Apps and Desktops, the boot device file is created automatically. Creating it automatically eliminates the need to boot using PXE. An unformatted write cache disk is automatically attached and formatted on first boot.
- When updating the Virtual Delivery Agent (VDA) on the virtual disk image, set the appropriate functional level for the Citrix Virtual Apps and Desktops catalog using the Citrix Virtual Apps and Desktops console. See the **Citrix Virtual Apps and Desktops upgrade** topics for more information.

- If you are importing an Active Directory .csv file, use the following format: `<name>,<type>,<description>`.
- The CSV file must contain the column header. For example, the csv file contents are: `Name,Type,Description,PVSPC01,Computer,,` The trailing comma must be present to signify three values, even if there is no description. The trailing comma format is the same formatting used by the Active Directory Users and Computers MMC when exporting the contents of an organizational unit.

SCVMM:

- The number of required connections for an SCVMM server is greater than or equal to the number of hosted hypervisors used by the setup wizard for virtual machine cloning. For example: to set connections to 25 from a PowerShell prompt, run: `winrm set winrm/config/winrs @{MaxShellsPerUser="25"}winrm set winrm/config/winrs @{MaxConcurrentUsers="25"}`
- For Microsoft SCVMM to support Citrix Virtual Apps and Desktops, run the following PowerShell command: `set-ExecutionPolicy unrestricted` on SCVMM. For Microsoft SCVMM, verify that the MAC address for the template is not 00-00-00-00-00-00 before attempting to clone the template.
- If necessary, use the **Template Properties** dialog to assign a MAC address.

More requirements:

- If you are running a vCenter server on alternate ports, the following registry modifications must be made to connect to it using Citrix Provisioning: **Create a new key** `HKLM\Software\Citrix\ProvisioningServices\PlatformEsx` - **Create a string in the Platform** ESX key named `ServerConnectionString` and set it to `<http://{0}:PORT#/sdk>`
- If you are using port 300, set ServerConnectionString=`<http://{0}:300/sdk>`.
- If you are using multiple NICs, the Citrix Virtual Apps and Desktops Setup Wizard assumes that the first NIC is the Citrix Provisioning NIC. The Setup Wizard changes it in accordance with the virtual machine network in the domain controller. This item is the first NIC listed in the virtual machines properties.
- To use the Synthetic switch-over feature, both the first legacy NIC and the synthetic NIC must be on the same network.
- If the Citrix Virtual Apps and Desktops setup wizard is used with SCVMM, both the first legacy and the synthetic NICs' network change according to the network resource. These NICs are set

by Citrix Virtual Apps and Desktops, or by the user if the SCVMM host has multiple network resources.

- Multi-NIC support exists for Citrix Virtual Apps and Desktops.
- Legacy Citrix Virtual Apps and Desktops agents are supported on VMs. For details, see VDA requirements in the Citrix Virtual Apps and Desktops documentation.

Streamed VM wizard setup

Streamed VM wizard requirements include:

- One or more hypervisor hosts must exist with a configured template.
- A device collection must exist in the Citrix Provisioning site.
- A virtual disk in standard image mode must exist, and must be associated with the selected VM template.

More requirements include:

Template VM:

- **Boot order:** Network/PXE must be listed first (as with physical machines).
- **Hard disks:** If you are using local write cache, an NTFS formatted disk large enough for the cache must exist. Otherwise, no hard disks are required.
- **Network:** Static MAC addresses. If you are using XenServer, the address cannot be 00-00-00-00-00-00. Before attempting to create a template from a VM, ensure that the VM is fully operational.

Permissions:

- The Citrix Provisioning console user account is added to a provisioning **SiteAdmin group** or above.
- If you are using Active Directory, when creating accounts in the console, they must possess the **Active Directory Create Accounts** permission. To use existing accounts, they must exist in a known OU for the selection.

ESD server requirements for virtual disk update management

ESD server requirements include:

- **WSUS server:** 3.0 SP2

- **SCCM:** SCCM 2016, SCCM 2012 R2, SCCM 2012 SP1, SCCM 2012

Hypervisor

The following sections include configuration information about supported hypervisors. For updated information on the supported versions, see CTX131239.

Citrix Hypervisor 5.6 and newer

The template MAC address cannot be 00-00-00-00-00-00-00-00.

Citrix Provisioning supports Citrix Hypervisor 8.1 functionality, guest UEFI boot, and secure boot. This functionality enables VMs running Windows 10 (64-bit), Windows Server 2016 (64-bit), or Windows Server 2019 (64-bit) to boot in UEFI mode. UEFI boot provides a richer interface for the guest operating systems to interact with the hardware, which can significantly reduce Windows VM boot times. See the XenServer documentation for more information.

XenServer

XenServer was formerly known as Citrix Hypervisor. XenServer 8 is the newer version of the product and contains the latest features and fixes. XenServer 8 is based on the same platform as Citrix Hypervisor 8.2 CU1 and so shares the same major version. For updated information on the supported versions, see CTX131239.

Secure boot in UEFI

Citrix Provisioning supports Secure Boot in UEFI on these platforms:

- Physical machines with UEFI firmware and the Secure Boot option.
- Hyper-V 2016 and later VMs that use the Microsoft UEFI Certificate Authority template in the **Secure Boot** setting. Hyper-V 2012 R2 is not supported.
- ESX version 6.7 or later, and 7.0 update 3.
- Nutanix AHV 6.5 LTS or later.
- XenServer 8.0 and Citrix Hypervisor 8.2 LTSR CU1
- Guest UEFI boot and secure boot for Citrix 8.1 Hypervisors are supported. See the XenServer documentation for more information.

Nutanix Acropolis

Nutanix Acropolis hypervisors are supported using the Citrix Virtual Apps and Desktops Setup Wizard. The following is **not** supported:

- Boot Device Manager (BDM) partition

For configuration information, see Deploying virtual desktops to VMs using the Citrix Virtual Apps and Desktops Configuration Wizard.

> **Important:**
>
> An Acropolis hypervisor (AHV) plug-in from Nutanix that supports Citrix Provisioning is required. Download this plug-in from the Nutanix support site. See the Nutanix documentation portal for installation information.

> Citrix Provisioning supports Windows 11 on Nutanix AHV 6.5 Long Term Support (LTS). Using Citrix Virtual Apps and Desktops Setup Wizard, you can create single and multi-session Nutanix AHV 6.5 catalogs. For more information on Nutanix AHV, see the following Nutanix documents:

- AHV Overview
- Securing AHV VMs with vTPM

System Center Virtual Machine Manager (SCVMM) VMM 2012 and newer

Consider the following when configuring this type of hypervisor:

- Microsoft System Center Virtual Machine Manager (SCVMM) 2019, 2022, and 2025 are supported.
- All Microsoft supported Windows 11 versions.
- VMM 2012, 2012 SP1, and 2012 R2 are different from each other.
- When creating a machine template for VMM 2012 only, ensure that it has a similar hard disk drive structure and that it can boot from a virtual disk in Private Image mode. Examples:
  - To PXE boot a VM with write cache, create a VM with one hard disk drive.
  - To use Boot Device Manager (BDM) to boot a VM with write cache, create a VM with two hard disk drives.

- For **Synthetic NIC Switch Over**, boot using legacy NIC and then stream using synthetic NIC, both the legacy and the synthetic NICs must be in the same VLAN in the template VMs. The **Citrix Virtual Apps and Desktops Set Up Wizard** changes the VLAN of both NICs to the VLAN selected when running the Wizard. This process uses two IP addresses.
- When running the imaging wizard, make sure you select the legacy NIC's MAC address.
- Citrix Provisioning does not support multiple legacy NICs in the VMM's VM. VMM uses the last legacy NIC. The Citrix Virtual Apps and Desktops Setup Wizard always uses the first NIC, regardless of whether it is legacy or synthetic.
- When creating a VMM template, make sure you select **None** – customization not required as the Guest OS profile in **Configure Operating System** menu.
- When using the Citrix Virtual Apps and Desktops Setup Wizard, the targets are created but are not bootable. An error appears **Device not found in the Citrix Provisioning database**. The reason is that the template has the legacy and synthetic NICs in reverse order: synthetic is NIC 1 and legacy is NIC 2. To resolve this issue, delete the NICs in the template. Make a legacy NIC 1 and synthetic NIC 2.

VMware vSphere ESX 6.7 and later

- **Supported Citrix Provisioning NIC**: Citrix Provisioning does not support E1000 emulated NIC types (including E1000, E1000E and so on). It is recommended for ESX environments that the VMXNET3 is used for optimal performance.
- **Template VM and the main VM:** Both must have the same guest operating system, configuration, and virtual machine version. Mismatches cause the process to stop unexpectedly.
- **Citrix Provisioning and ESX VM version:**
  - The virtual machine version must be changed before OS installation.
  - The template and the main VM must have the same virtual machine version.
  - Citrix Provisioning supports ESX 6.7 and later.
  - All Microsoft supported Windows 11 versions.
  - Citrix Provisioning supports VMware vSAN 8.0. You can upgrade your existing vSAN environment to vSAN 8.0.
- **ESX:**

    - When using multiple NICs in ESX VM, the order of the NICs in the VM's properties, BIOS, and OS differ. Consider this configuration when making your choices for the streaming NIC. This is the first NIC in the VM's properties. You can choose the **PXE NIC** in the BIOS.

- **Host record:** Regardless of the ESX version, the host's address for the Citrix Virtual Apps and Desktops host is the vCenter system. Do not enter the address used by the web client.

Support for Single Root I/O Virtualization (SR-IOV)

Citrix Provisioning supports client using SR-IOV on the following hypervisors:

- Hyper-V
- VMware vSphere
- Azure

> **Note:**
>
> For information specific to Citrix Provisioning on Microsoft Azure, see Citrix Provisioning on Microsoft Azure.

Support for cloud platforms

Citrix Provisioning supports the following cloud platforms:

- Citrix Provisioning on Microsoft Azure
- Citrix Provisioning on Google Cloud Platform
- Citrix Provisioning in Nutanix on AWS
- VMware cloud and partner solutions: The following VMware cloud variants are supported:
    - Azure VMware Solution (AVS) integration
    - VMware Cloud on AWS
    - Google Cloud VMware Engine

> **Note:**
>
> The VMware cloud variants are supported from Citrix DaaS™ (formerly Citrix Virtual Apps and Desktops service) or if you have a Hybrid Rights License.

Licensing

Citrix Provisioning is available under the Citrix Virtual Apps and Desktops™ entitlement, and is licensed per target device. Each provisioned target device checks out a single Citrix Provisioning license (included with your Citrix Virtual Apps and Desktops license file).

Citrix Provisioning™ is also available under the DaaS entitlement. You can obtain a special Citrix Provisioning license file that is installed into the License Server. Configure the Citrix Provisioning licensing to use **Cloud** type licenses irrespective of where Citrix Provisioning is running.

The Citrix License Server must be installed on a server that can communicate with all Citrix Provisioning servers within the farm. You need one license server per Citrix Provisioning farm. You can use the same license server for multiple Citrix Provisioning farms. The total license count is shared between the farms.

Use the most recent version of the Citrix License Server to receive the latest provisioning features. If you are upgrading Citrix Provisioning to the newest version, the latest License Server version is required. When you do not upgrade to the latest version of the License Server, the product license enters the 30-day License caching mode.

Important:

- Provisioning servers must be connected to the license server to operate successfully. Use the most recent version of the Citrix License Server to get the latest features. Citrix recommends that you upgrade the License Server **before** upgrading Citrix Provisioning to avoid any licensing conflicts related to License caching modes.
- As outlined in Required License Server Update, Cloud Software Group has updated the licensing requirements that require you to upload telemetry. With this implementation, you must return and reallocate your Citrix Virtual Apps and Desktops and Citrix Provisioning 1912 LTSR CU8 and later CUs, 2203 LTSR CU3 and later CUs, 2305 and later, and 2402 LTSR and later CUs. This reallocation of licenses does not apply to Citrix DaaS customers who only have `PVS_CCLD_CCS` license.
- According to the updated licensing requirements, Citrix Provisioning now attempts to check out a Citrix Provisioning license for each target. When you return and re-allocate your licenses, you get a license file that includes all the required Citrix Provisioning licenses based on your Citrix Provisioning entitlement. No other changes are included in

this license file. Therefore, if you reallocate the licenses, you can avoid any possible licensing issues.

Consider the following options when deciding which server to use as the license server:

- Single system: install the license server on the same system as Citrix Provisioning. This option is suitable for evaluations, test labs, or implementations with one Citrix product.
- Stand-alone: install the license server on a separate system. This option is suitable for larger implementations or implementations using multiple Citrix products.
- Point to an existing license server.

For detailed Citrix licensing information, see Licensing.

For information related to virtual disk volume licensing, see Configuring a vDisk for Microsoft Volume Licensing.

Required license types

After you reallocate your licenses as per the updated licensing requirements, you have the following licenses in your licensing file.

Note:

The updated license requirement does not apply to Citrix DaaS™ customers who only have `PVS_CCLD_CCS` license.

	VIRTUAL DESKTOPS STANDARD	VIRTUAL APPS ADVANCED	VIRTUAL APPS PREMIUM	VIRTUAL APPS AND DESKTOPS ADVANCED	VIRTUAL APPS AND DESKTOPS PREMIUM
Expected licenses	PVSD_STD_CCS	PVSD_STD_CCS	PVSD_STD_CC and PVS_STD_CCS	PVSD_STD_CCS and	PVSD_STD_CCS and

	VIRTUAL DESKTOPS STANDARD	VIRTUAL APPS ADVANCED	VIRTUAL APPS PREMIUM	VIRTUAL APPS AND DESKTOPS ADVANCED	VIRTUAL APPS AND DESKTOPS PREMIUM
				PVS_STD_CCS	PVS_STD_CCS

If you upgrade your license to Universal Hybrid Multi Cloud License (UHMC) or Platform License (UPL), you receive an on-premises universal license file which contains `PVS_CCS` and `PVSD_CCS` licenses. To configure your new licenses, run the Configuration Wizard to change the license type from **Cloud** to **On-premises** on the **License Server** page.

License caching modes

There are two types of License caching modes:

- **Out-of-box License caching mode** is 30 days (720 hours). Initial installation of the licensing server provides startup licenses for all Citrix products. Startup licenses expire after 30 days. The 30-day countdown begins when the product prompts you for the startup license for the first time. Citrix Provisioning product licenses must be installed during this period. A startup license for a Citrix product is voided if a license for that product is installed.
- **License server connectivity outage License caching mode** is 30 days (720 hours). If connectivity to the Citrix License Server is lost, Citrix Provisioning continues to provision systems for 30 days.

When Citrix Provisioning is in a License caching mode, you are notified through a message in the Event Viewer of the Citrix Provisioning server.

When a License caching mode expires, targets display popups indicating they are not licensed and shut down in a further 30 days if licensing is not re-established.

Important:

When you upgrade an existing environment to the newest version of Citrix Provisioning, also upgrade to the latest version of the licensing server or the product license. Failure to perform this upgrade results in Citrix Provisioning entering a 30-day License caching mode.

Installing the license server

Download the latest version of Citrix Licensing from the download page at `<http://www.citrix.com/downloads/licensing.html>`.

> **Note:**
>
> Restart the stream service if Citrix Provisioning is installed after the license server, or if new licenses are added.

Specify a license to communicate with the license server

Use the Configuration Wizard to specify a license. For information, see Select the license server.

Alternately, view or change the license type on the **Farm Properties** screen. For information, see Licensing tab.

Using accelerated Microsoft office activation

An administrator can force the immediate activation of a Microsoft Office license once a system starts up. In previous releases, a provisioned virtual disk activates a license when the virtual machine boots. This lengthy background process occurred after the VM reaches the **Citrix Virtual Apps™ and Desktops login** screen. As a result, users encounter licensing conflicts that would lead them to believe a license did not exist for the VM.

To access this new feature:

- use **Microsoft Volume Licensing** tab in the virtual disk Properties screen. Click the **Key Management Service (KMS)** radio button, then click the **Accelerated Office Activation** check box. Select **OK** to apply the configuration change to the virtual disk.



- use the Citrix Provisioning Imaging Wizard. In the **Microsoft Volume Licensing** screen, click the appropriate license management option for the virtual disk. Click the **Key Management Service (KMS)** radio button, then click the **Accelerated Office Activation** check box. Select **Next** to apply the configuration change to the virtual disk and continue configuring the virtual disk.



Tip:

For implementations using Microsoft Active Directory, set the **Microsoft Volume Licensing** option in the vDisk property to **None**. If the operating system meets the requirements set by Microsoft, Windows activates automatically. For additional information and prerequisites for Windows Active Directory, see Activate using Active Directory-based activation.

Hybrid Rights License with Citrix licensing server

Citrix Provisioning now allows the following using Hybrid Rights License with Citrix licensing server:

- You can work with on-premises (customer-managed delivery controller™) when running Citrix Provisioning in Azure.
- You must have Citrix Virtual Apps and Desktops license with Hybrid Rights when running Citrix Provisioning in Azure.

Note:

- Citrix Provisioning running in Azure does not support creating sites or provisioning targets in on-premises hypervisors.
- Citrix Provisioning running in on-premises does not support creating sites or provisioning targets in Azure.

The following table describes the support for Hybrid Rights License with Citrix licensing server:

OWNED LICENSE	DELIVERY CONTROLLER	LICENSE AVAILABLE	SUPPORTED HYPERVISOR
On-premises Citrix Virtual Apps and Desktops	Customer managed	License file has Citrix Virtual Apps and Desktops licenses	On-premises hypervisors only. No support for running in Azure.
Citrix DaaS	Citrix Cloud™	License file has Citrix Provisioning Cloud licenses	On-premises and cloud hypervisors. Citrix Provisioning

OWNED LICENSE	DELIVERY CONTROLLER	LICENSE AVAILABLE	SUPPORTED HYPERVISOR
			running in Azure is allowed.
Hybrid Rights License	Customer managed	License file has Hybrid Rights License	On-premises and cloud hypervisors.
Hybrid Rights License	Citrix Cloud	License file has Hybrid Rights License	On-premises and cloud hypervisors.

Effect of Hybrid Rights License on host connection

There are three scenarios where the host connection to the public cloud hosts is affected based on Hybrid Rights License entitlement:

- To create a new host connection to the public cloud hosts, you must have Hybrid Rights License.
- If you have Hybrid Rights License but the license has expired, then the existing connections to public cloud hosts are marked as not entitled and enter into maintenance mode. When existing host connections are in maintenance mode, you cannot do the following:
  - Add or modify host connections
  - Create catalog and update image
  - Perform power actions
- If a new Hybrid Rights License is installed, existing hosting connections are re-enabled.

Citrix Provisioning™ telemetry data elements

Citrix Provisioning 2402 LTSR CU1 telemetry data elements

Headers

KEY	DESCRIPTION	EXAMPLE
ver	Indicates the version of the license usage event.	1.0
id	Indicates a unique identifier of the usage event.	d4ce7919-5d80-44de-a8fa-102923fe0ead
type	Indicates the event type used by Citrix Analytic Service to identify cloud usage events.	Cloud.Licensing
st	Indicates the UTC timestamp when the event is generated in Citrix Provisioning.	2011-08-12T20:17:46.384Z
prod	Identifies the originating product and deployment of the usage event.	XenDesktop.PVS
prodVer	Indicates the Citrix Provisioning product version.	7.40.0.10
dvc.dvcId	Indicates the device ID to uniquely identify a device.	0123456789ABCDEF
dvc.dvcName	Indicates the friendly name for the device. **The value is scrambled.**	E6oNXGy6fihiwi6cHdS/sg== **(always scrambled)**

Payload

KEY	DESCRIPTION	EXAMPLE
licenseActivityTimeStamp	Indicates the UTC timestamp when the payload is generated.	2011-08-12T20:17:46.384Z

KEY	DESCRIPTION	EXAMPLE
deviceId	Indicates the target device ID (GUID).	d4ce7919-5d80-44de-a8fa-102923fe0ead
ver	Indicates the payload version	1.0
droppedEvents	Indicates that the count of events dropped since the last event sent.	0
licenseActivityType	Indicates the licensing event type.	DeviceStart
os	Indicates the type of the OS.	Windows or Linux
osType	Indicates whether the target is desktop or server.	Desktop
workerSid	Indicates a unique identifier for the Virtual Delivery Agent (VDA) used for the session. **The value is scrambled.**	GF/5+DT7Hb7DJIvIW+bYQA== **(always scrambled)**
vDiskId	Indicates the identity of the vDisk that is being streamed. The value includes the id and version in the `id:version` format.	24d03af2-92a7-4063-813d-75fa84fe64dd:2
hypervisorType	If known, this value indicates the type of Hypervisor used.	Azure

KEY	DESCRIPTION	EXAMPLE
ramSize	Indicates the maximum size of RAM cache (MB)	32
cacheType	Indicates the type of cache that's in use.	10
enabledFeatures	Indicates the features that are enabled for the session for metering. The value is either true or false for each feature.	enabledFeatures: { subnetAffinity: false rebalanedEnabled: false asynchronousIoEnabled: true cachedSecretsCleanupEnabled: true maintenanceMode: false dbOfflineFeatureEnabled: true dbOffline: false}

Citrix Provisioning 2402 LTSR CU2 telemetry data elements

In addition to the telemetry data elements in 2402 CU1, there is a new record type in 2402 CU2 called FarmMetrics that has the following format:

Header

KEY	DESCRIPTION	EXAMPLE
ver	Indicates the version of the license usage event.	1.0
id	Indicates the unique identifier of the usage event.	d4ce7919-5d80-44de-a8fa-102923fe0ead

KEY	DESCRIPTION	EXAMPLE
type	Indicates event type used by CAS to identify cloud usage events.	Metrics
st	Indicate the timestamp when the event is generated in PVS.	2011-08-12T20:17:46.384Z
prod	Identifies the originating product and deployment of the usage event.	XenDesktop.PVS
prodVer	Indicates the PVS product version.	7.40.0.10

Payload

The payload portion contains the following fields:

KEY	DESCRIPTION	EXAMPLE
farmId	Indicates the Farm ID (GUID)	d4ce7919-5d80-44de-a8fa-102923fe0ead
ver	Indicates the version of the payload.	1.0
metricsType	Indicates the metrics event type.	FarmMetrics
siteCount	Indicates the number of sites in farm	2
serverCount	Indicates the number of PVS servers in farm	10
diskCount	Indicates the number of vDisks that exist	30

Configuring a vDisk for Microsoft Volume Licensing

Configure a vDisk for Microsoft Key Management Service (KMS) or Multiple Activation Key (MAK) volume licensing when running the Imaging Wizard. If the vDisk was not configured using the Imaging Wizard, it can still be configured from the Citrix Provisioning™ console.

> **Important:**
>
> Citrix Provisioning does not support MAK activation for Microsoft Office products.

Using MCLI and SOAP server command line interfaces for Microsoft volume licensing

MCLI and SOAP Server command-line interfaces can be used to configure Microsoft Volume Licensing using the following procedure:

1. Select the vDisk in the Citrix Provisioning console, then right-click and select **File Properties**. The **vDisk File Properties** dialog appears.
2. Click the **Microsoft Volume Licensing** tab, then select the **MAK** or **KMS** licensing method.
3. Click **OK**.

Configuring Microsoft KMS volume licensing

This section describes how to use KMS license access codes with Citrix Provisioning.

> **Note:**
>
> Support for KMS licensing requires the SOAP Server user account is a domain user with the right to perform volume maintenance tasks. The domain user is typically found in `Local\\Computer Configuration\\Windows Settings\\Security Settings\\Local Policies\\User Rights Assignment`. By default, a member of the local administrators group has this right.

> KMS volume licensing utilizes a centralized activation server. This server runs in the data center, and serves as a local activation point (opposed to having each system activate with Microsoft over the internet).

> **Note:**
>
> Preparing or updating a KMS configured vDisk that is copied or cloned includes completing the final configuration task. Change the vDisk mode from **Private Image Mode** to **Shared Image Mode**. Prepare the vDisk before copying or cloning the vDisk to other Provisioning Servers. Copy the `pvp` and `vhdx` file to retain the properties and KMS configuration of the original vDisk.

The tasks involved in configuring a vDisk image to use KMS volume licensing and managing that vDisk in a Citrix Provisioning farm includes:

- Enabling KMS licensing on the created vDisk. Select the **KMS** menu option on the Microsoft Volume Licensing tab when running the Imaging Wizard. See the Imaging Wizard for details.
- Preparing the new base vDisk image
- Maintaining or upgrading the vDisk image

Note: If KMS licensing was not configured on the vDisk when running the Imaging Wizard, alternatively configure it using the Console. You can also configure it using the MCLI and PowerShell command-line interface.

Preparing the new base vDisk image for KMS volume licensing

After you create a vDisk using the Imaging Wizard, it must be reset to a non-activated state using the **rearm** command.

Perform this operation on a system booted from the vDisk in **Private Image Mode**. This process ensures that the master target device hard disk's rearm count is not reduced.

Tip: Microsoft limits the number of times you can run rearm on an installed OS image. Reinstall the operating system if you exceed the number of allowed rearm attempts.

1. Boot the target device from the vDisk in private image mode to rearm.

   > **Note:**
   >
   > OSPPPREARM.EXE must be run from an elevated command prompt.

2. A message prompts you to reboot the system, DO NOT REBOOT. Instead shut down the target device.
3. If the KMS option was not selected when the vDisk image was created, click the **Microsoft Volume Licensing** tab and set the licensing option to **KMS**.
4. Set the vDisk mode to standard image mode.
5. Stream the vDisk to one or more target devices.

Use the information in the following sections to configure various KMS scenarios.

Maintaining or upgrading a vDisk image that uses KMS volume licensing

To maintain or upgrade a vDisk image that is configured to use KMS volume licensing:

1. Set the vDisk mode to **Private Image mode**.
2. Stream the vDisk to a target device.
3. Apply the OS/application service pack/update, then shut down the target device.
4. Set the vDisk mode back to **Shared Image mode**.
5. Stream the vDisk to the target device in shared image mode. **Note:** If Office 2010 is installed as a vDisk update, or after the vDisk has gone through the base disk preparation process once, repeat the base disk preparation using the following procedure:

    a. In the Citrix Provisioning console, right-click on the vDisk, then select the **File Properties** menu option. The **vDisk File Properties** dialog appears.

    b. Click the **Microsoft Volume Licensing** tab, then change the licensing option from **KMS** to **None**.

    c. On the **Mode** tab, set the vDisk access mode to **Private Image mode**.

    d. PXE boot to the vDisk in private image mode to rearm. **Note:** OSPPPREARM.EXE must be run from an elevated command prompt.

    e. A message prompts you to reboot the system, DO NOT REBOOT. Instead shut down the target device.

    f. In the console, right-click the vDisk you are configuring, then select the **File Properties** menu option. The **vDisk Properties** dialog appears.

    g. Click the **Microsoft Volume Licensing** tab, then change the license option from **None** to **KMS**.

    h. On the **Mode** tab, set the vDisk access mode to **Shared Image mode**.

    i. Stream the vDisk to the target devices.

Maintaining or upgrading a vDisk image enabled with versioning that is currently using KMS

In this scenario, a vDisk is already configured for KMS and is deployed successfully. The disk is enabled to use *vDisk versioning*, so versions can exist. Consider:

- For both Microsoft Windows and Microsoft Office: A vDisk is already configured for KMS and is deployed successfully.
- For environments with only Microsoft Windows or only Microsoft Office: The vDisk is already configured for KMS *Only Windows* or *Only Office* and is deployed successfully.

To maintain or upgrade the vDisk:

1. In the Citrix Provisioning console, right-click the virtual disk, and select **Versions**.
2. Create a disk version.
3. Access the target device properties and set **Type** to **Maintenance**.
4. Start the target device.
5. Access the target device machine and select **Maintenance** from the **Boot** menu when prompted.
6. Select the required operating system in **Application/Service Pack/Update**.
7. Shut down the target device.
8. Access the Citrix Provisioning console, select the vDisk and right-click to display the contextual menu.
9. Select **Versions**. Promote the vDisk from **Maintenance** to **Production** or **Test**.
10. Access the Citrix Provisioning console. Under **Target device properties**, change the **Type** to **Production** or **Test**.

Stream the vDisk with this version to one or more target devices.

Installing Microsoft Office to an existing KMS configured vDisk during Maintenance

A vDisk already uses KMS, is configured for Microsoft Windows and is deployed successfully.

To install Microsoft Office to a vDisk during maintenance:

1. In the Citrix Provisioning console, right-click on the vDisk and select **Properties**.
2. Select the **Microsoft Volume Licensing** tab and change the licensing option from **KMS** to **None**.

3. On the **General** tab, set the vDisk access mode to **Private Image** mode.
4. PXE boot to the vDisk in Private Image mode to rearm:
    a. For Office (for 64-bit client): `Program Files(x86)\Common Files\microsoft shared\OfficeSoftwareProtectionPlatform\OSPPREARM.EXE`
    b. For Office (for 32-bit client): `Program Files\Common Files\microsoft shared\OfficeSoftwareProtectionPlatform\OSPPREARM.EXE`
    c. Repeat for other Windows versions: Run `cscript.exe slmgr.vbs –rearm`
5. A message is displayed to reboot the system. Do not reboot. Instead, shut down the target device.
6. In the console, right-click the vDisk and select **Properties**.
7. Select the **Microsoft Volume Licensing** tab and change the license option from **None** to **KMS**.
8. On the **General** tab, set the vDisk access mode to **Standard Image** mode.
9. Stream the vDisk to one or more target devices.

> **Tip:**
>
> You can validate the KMS configuration by verifying that the `CMID` for each device is unique. For Windows versions, run `cscript.exe slmgr.vbs –dlv`. For Office versions, run `C:\Program Files\Microsoft Office\Office14\cscript ospp.vbs /dcmid`.

Important information on rearm

Consider the following when rearming:

- Microsoft limits the number of times you can run rearm on an installed operating system image and Microsoft Office. The operating system and Office image must be reinstalled accordingly if you exceed the number of allowed rearm attempts.
- For a successful KMS configuration using a Citrix Provisioning vDisk, you are not required to rearm the disk except the first time when you configure it.
- Citrix® recommends that you rearm the system that is started from the vDisk in **Private Image** mode. This ensures that the rearm count of the master target device hard disk is not reduced.

Installing Microsoft Office to an existing KMS configured for a Windows vDisk

A vDisk is already configured for KMS using Microsoft Windows and is deployed successfully. To install Microsoft Office to an existing KMS that is configured for Microsoft Windows:

1. In the Citrix Provisioning console, right-click the vDisk and select **Properties**.
2. Select the **Microsoft Volume Licensing** tab and change the licensing option from **KMS** to **None**.
3. On the **General** tab, set the **vDisk Access Mode** to **Private Image** mode.
4. PXE boot to the vDisk in **Private Image** mode to rearm. An OS rearm is required along with the Microsoft Office rearm.
    a. For Microsoft Windows, run `cscript.exe slmgr.vbs -rearm`.
    b. For Microsoft Office 2010, run `%ProgramFiles%\Common Files\MicrosoftShared\OfficeSoftwareProtectionPlatform\OSPPREARM.EXE`.
    c. For Microsoft Office 2013 and 2016, run `%ProgramFiles%\Microsoft Office\%Office%\OSPPREARM.EXE`.
5. A message is displayed to reboot the system. Do not reboot. Instead, shut down the target device.
6. In the console, right-click the vDisk and select **Properties**.
7. Select the **Microsoft Volume Licensing** tab and change the license option from **None** to **KMS**.
8. On the **General** tab, set the **vDisk Access Mode** to **Standard Image** mode.
9. Stream the vDisk to one or more target devices.

You can validate the KMS configuration by verifying that the `CMID` for each device is unique. For Windows versions, run `cscript.exe slmgr.vbs –dlv`. For Office versions, change the directory to `%ProgramFiles%\Microsoft Office\%Office%` and then run:

- `cscript ospp.vbs /dcmid`
- `cscript ospp.vbs /dstatus`. The OS and Microsoft Office discovery of KMS is independent from each other. `/dstatus` appears if Microsoft Office has located KMS on the network.
- `cscript ospp.vbs /act`. This command expedites the activation process.

Upgrading Microsoft Office on an existing KMS configured for a Microsoft Windows vDisk

A vDisk is already configured for KMS that uses Microsoft Windows and Microsoft Office. To upgrade:

1. In the Citrix Provisioning console, right-click on the vDisk and select **Properties**.
2. On the **General** tab, set the **vDisk Access Mode** to **Private Image** mode.
3. Start the target device.
4. Run the new Microsoft Office setup. Choose to perform an upgrade.
5. Reboot the target device as required by the installation.
6. Shut down the target device.
7. Connect to the Citrix Provisioning Server. In the console, right-click on the vDisk and select **Properties**.
8. On the **General** tab, set the **vDisk Access Mode** to **Standard Image** mode.
9. Stream the vDisk to one or more target devices.

Important information on rearm

- Microsoft limits the number of times you can run rearm on an installed operating system image and Microsoft Office. The operating system and Office image must be reinstalled accordingly if you exceed the number of allowed rearm attempts.
- For Windows and Office products utilizing KMS activation, the available rearm count increments from 0 to 1 on a successful activation against a KMS host server.
- If you run out of rearms, activating by using a KMS host lets you rearm once. This ensures that once you activate a KMS client, they can issue a rearm. For example, a KMS client with a rearm count of 1 issues a rearm using the remaining single rearm, and reboots. Upon reboot after the KMS client activates, the rearm count will return to a count of 1.

> **Tip:**
>
> A successful KMS configuration for a Citrix Provisioning vDisk does not require you to rearm the vDisk except the first time when it is configured.

Configuring Microsoft MAK volume licensing

This section describes the use of Multiple Activation Keys (MAK). A MAK corresponds to some purchased OS licenses. The MAK is entered during the installation of the OS on each system. The installation activates the OS and decrements the count of purchased licenses centrally with Microsoft. Alternatively, a process of *proxy activation* is done using the Volume Activation Management Toolkit (VAMT). Proxy activation works on systems that do not have access to the Internet. Citrix Provisioning applies this proxy activation mechanism for standard image mode vDisks that have the MAK licensing mode selected when creating the disk.

The Volume Activation Management Tool (VAMT) version 3.1 must be installed and configured on all provisioning servers within a farm. This tool is available from the Microsoft Windows Assessment and Deployment Kit (Windows ADK). For more information, see Install VAMT.

When you first run the VAMT, a VAMT database is created. This database caches all device activations and allows for the reactivation of Citrix Provisioning.

Volume Activation Management Tool 3.1 requires:

- PowerShell 3.0 or later – the OS is newer than Windows Server 2012 or Windows 8
- SQL 2012 express or newer

Citrix Provisioning MAK activation requires you to configure one of three user types:

- **Volume Activation Management Tool/Provisioning Services installation user** — This user is a local administrator possessing rights on SQL 2012 or newer (VAMT 3.1 requirement). These rights are used to create a database for VAMT.
- **MAK user** — The user defined in the site's properties. This user handles the MAK activation on both server and client side. This user is a local administrator on both the provisioning server and the master client. This user requires full access to the VAMT database.
- **Citrix Provisioning SOAP/stream services user** — the stream process handles the reactivation when the target device restarts. This user requires read access to the VAMT database.

Provisioning servers use PowerShell to interface with the VAMT. These manual configuration steps are required one time per server:

1. Install PowerShell 3.0 or later.
2. Install VAMT 3.1 on every provisioning server system using a Volume Activation Management Tool/Provisioning Services installation user.

3. Configure a VAMT database as prompted during the initial run of VAMT 3.1. Make this database accessible to all provisioned servers used to stream VAMT activated Citrix Provisioning target devices.
4. If the user who created the VAMT database is not the SOAP/stream service user, copy the VAMT configuration file `C:\\Users\\\<VAMT installation user (dB creator)\>\\AppData\\Roaming\\Microsoft\\VAMT\\VAMT.config` to `C:\\Users\\\<Provisioning Services soap/stream services user\>\\AppData\\Roaming\\Microsoft\\VAMT\\VAMT.config`.
5. Set the provisioning server security configuration to use PowerShell to interface with VAMT.
    a. Set-ExecutionPolicy -Scope \ (the Provisioning Services services user) to *unrestricted* – see Set-ExecutionPolicy for more information.
    b. WinRM quickconfig.
    c. Enable-WSManCredSSP -Role Client -DelegateComputer \<this server fqdn> -Force
    d. Enable-WSManCredSSP -Role Server –Force.
6. Configure the Windows firewall on the client for VAMT 3.1 – see Configure Client Computers for more information. Citrix Provisioning target devices cannot be activated or reactivated if the firewall is not configured for VAMT.

Common activation errors

Error: Failed to create PSSession — Reason: MAK user is not a local administrator on the Citrix Provisioning server.

Error: Index was out of range. Must be non-negative and less than the size of the collection. Parameters name: Index.

Reason: MAK user does not have full access (read\write) permission to the VAMT database.

Setting the vDisk licensing mode for MAK

A vDisk can be configured to use Microsoft Multiple Activation Key (MAK) licensing when running the Imaging Wizard. If MAK licensing was not configured when running the Imaging Wizard, the vDisk's licensing mode property can be set using the console, MCLI, or PowerShell user interface. The licensing mode is set before activating target devices.

Note: For information on using the command-line interfaces, see the MCLI or PowerShell Programmers Guide.

Entering MAK user credentials

Before target devices that use MAK-enabled vDisks can be activated, MAK user credentials must be entered for a site.

Note: The user must have administrator rights on all target devices that use MAK-enabled vDisks, and on all Provisioning Servers that stream the vDisks to target devices.

To enter credentials:

1. Right-click on the site where the target devices exist, then select the **Properties** menu option.
2. On the **MAK** tab, enter the user and password information in the appropriate text boxes, then click **OK**.

Activating target devices that use MAK-enabled vDisks

After a vDisk is configured for MAK volume licensing, each target device assigned to the vDisk must be activated with a MAK.

Note: After all licenses for a given MAK are used, a new key is required to allow more target devices to share this vDisk image.

To activate target devices that use MAK volume licensing from the Console:

1. Boot all target devices that are to be activated.
2. In the Console, right-click on the collection or view of the individual device including those target devices requiring MAK license activation. Select the **Manage MAK Activations...** menu option. The **Manage MAK Activations** dialog appears.
3. In the **Multiple activation key** text box, enter the **MAK** to activate the target devices.
4. The number of booted target devices requiring activation display on the dialog. From the list of booted devices, check the box next to each target device that you want to activate.
5. Click **OK** to activate licensing for all selected target devices. Do not close the dialog until the activation process is completed. The process can be stopped by clicking the **Cancel** button. Closing the dialog before the activation process completes stops the process might result in some target devices not being activated. The **Status column** indicates if a target device is being activated or failed. If all target devices were activated successfully, click **OK** to close the dialog. If one or more target devices are not activated, or if devices were not activated successfully, the dialog displays any unactivated devices. After resolving any issues, repeat this step to activate the remaining target devices.

> **Note:**
>
> The **Manage MAK Activations** option does not display after all currently booted target devices have been successfully activated.

Maintaining MAK activations

Typically, devices and their assigned vDisk activations are preserved automatically. When a different target device is assigned a MAK activated vDisk, it removes any saved existing MAK reactivation information. If the vDisk is reassigned in the future, the target device fails to reactivate. To prevent the loss of MAK activation, do not unassign the activated disk from the target device.

To change a target device's vDisk, without losing the MAK activation, select one of the following methods:

- Assign more vDisks to the target device, without removing any, then set the default booting vDisk accordingly.
- Assign more vDisks to the target device and temporarily disable the MAK activated vDisk.

For you to update a MAK activated vDisk, the **Auto Update** feature must be used so that the MAK activation information is maintained. This process is required for the shared device reactivation.

More MAK considerations:

- Manual vDisk updates (unassigning one vDisk and reassigning another vDisk) results in the loss of the required MAK activation information. This process requires a new activation, which would consume another license.
- Using auto update to deploy a new vDisk from a different OS results in mismatched MAK activation information. In this case, a new activation must be performed from the command line interface, as only unactivated target devices can be activated from the Citrix Provisioning console.

Architecture

Most enterprises struggle to keep up with the proliferation and management of computers in their environment. Each computer, whether it is a desktop PC, a server in a data center, or a kiosk-type device, must be managed as an individual entity. The benefits of distributed processing come at the cost of distributed management. It costs time and money to set up, update, support and ultimately decommission each computer. The initial cost of the machine is surpassed by operating costs.

Citrix Provisioning™ takes a different approach from other imaging solutions by changing the relationship between hardware and the software that runs on it. By streaming a single shared disk image, a virtual disk, rather than copying images to individual machines, Citrix Provisioning offers the following benefits:

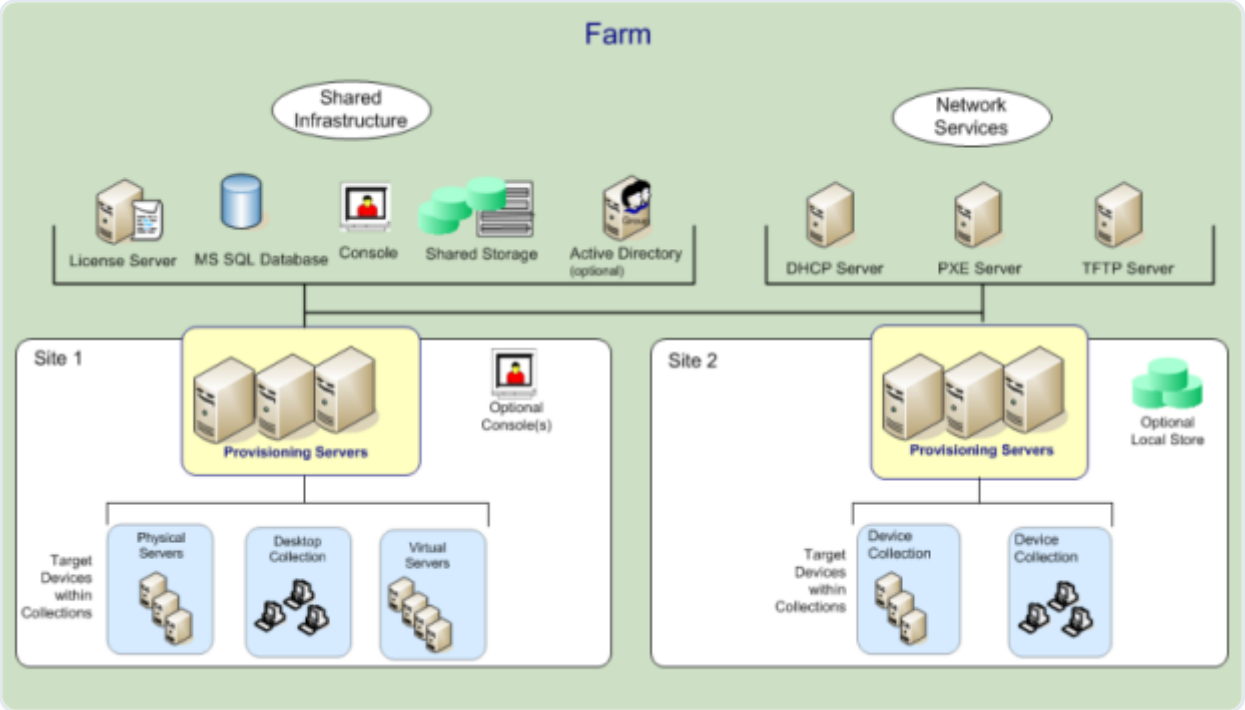
- Enables organizations to reduce the number of disk images that they manage, even as the number of machines continues to grow.
- Provides the efficiencies of a centralized management solution with the benefits of distributed processing.

In addition, because machines are streaming disk data dynamically from a single shared image, machine image consistency is ensured. At the same time, large pools of machines can completely change their configuration, applications, and even operating systems in the time it takes them to reboot.

How Citrix Provisioning works

Using Citrix Provisioning, any virtual disk can be configured in *standard image mode*. Standard image mode allows many computers to boot from it simultaneously, greatly reducing the number of images that must be maintained and the amount of required storage. The virtual disk is in a read-only format. Target devices cannot change the image.

The following image provides a high-level view of a basic Citrix Provisioning infrastructure and shows how provisioning components might appear within that implementation.



Benefits to Citrix Virtual Apps and Desktops™ and other server farm administrators

If you manage a pool of servers that work as a farm, such as Citrix Virtual Apps™ and Desktops servers or web servers, maintenance is problematic. Maintaining a uniform patch level on your servers can be difficult and time consuming. With traditional imaging solutions you start out with a pristine golden master image. But when a server is built with the master image, you now must patch the individual server along with the other servers. Rolling patches out to individual servers in your farm is inefficient and unreliable. Patches often fail on an individual server. Problems are not realized until users have conflicts or the server has an outage. Once that happens, getting the server back into sync with the rest of the farm is challenging and sometimes requires a full reimaging of the machine.

With Citrix Provisioning, patch management for server farms is simple and reliable, you start out managing your golden image and you continue to manage that single golden image. All patching is done in one place and then streamed to your servers when they start. Server build consistency is assured because all your servers are using a single shared copy of the disk image.

If a server becomes corrupted, reboot it and it's instantly back to the known good state of your master image. Upgrades are fast. Once you have your updated image ready for production you assign the new image version to the servers and reboot them. In the time it takes machines to reboot you can deploy the new image to any number of servers. Roll-backs can be done in the

same manner so problems with new images do not impact your servers or your users for an extended time.

Benefits for desktop administrators

With Citrix Virtual Apps and Desktops, desktop administrators use Citrix Provisioning streaming technology to simplify, consolidate, and reduce the costs of both physical and virtual desktop delivery. Many organizations are exploring desktop virtualization. While virtualization addresses many of the consolidations and simplified management needs of IT, configuring it also requires the deployment of supporting infrastructure. Without Citrix Provisioning, storage costs can put desktop virtualization out of the budget. With Citrix Provisioning, IT can reduce the amount of storage required for VDI by as much as 90 percent. At the same time the ability to manage a single image rather than hundreds or thousands of desktops significantly reduces the cost, effort, and complexity for desktop administration.

Different types of workers across the enterprise need different types of desktops. Some require simplicity and standardization, while others require high performance and personalization. Citrix Virtual Apps and Desktops can meet these requirements in a single solution using FlexCast™ delivery technology. With FlexCast™, IT can deliver every type of virtual desktop - each tailored to meet the performance, security, and flexibility requirements of each individual user.

Not all desktop applications are supported by virtual desktops. For these scenarios, IT can still reap the benefits of consolidation and single image management. Desktop images are stored and managed centrally in the data center and streamed out to physical desktops on demand. This model works well for standardized desktops such as those in lab and learning environments, call centers, and "thin client" devices used to access virtual desktops.

The Citrix Provisioning solution

Citrix Provisioning streaming technology allows computers to be provisioned and reprovisioned in real time from a single shared-disk image. Using a single shared image enables administrators to completely eliminate the need to manage and patch individual systems. Instead, all image management is done on the master image. The local hard disk drive of each system is used for runtime data caching. In some scenarios, the disk is removed from the system entirely, which reduces power usage, system failure rates, and security risks.

The Citrix Provisioning infrastructure is based on a software-streaming technology. After you install and configure Citrix Provisioning components, a virtual disk is created from a device’s hard drive. This disk is created by taking a snapshot of the OS and application image, and then storing that

image as a virtual disk file on the network. The device that is used during this process is seen as a master target device. The devices that use those vDisks are called target devices.

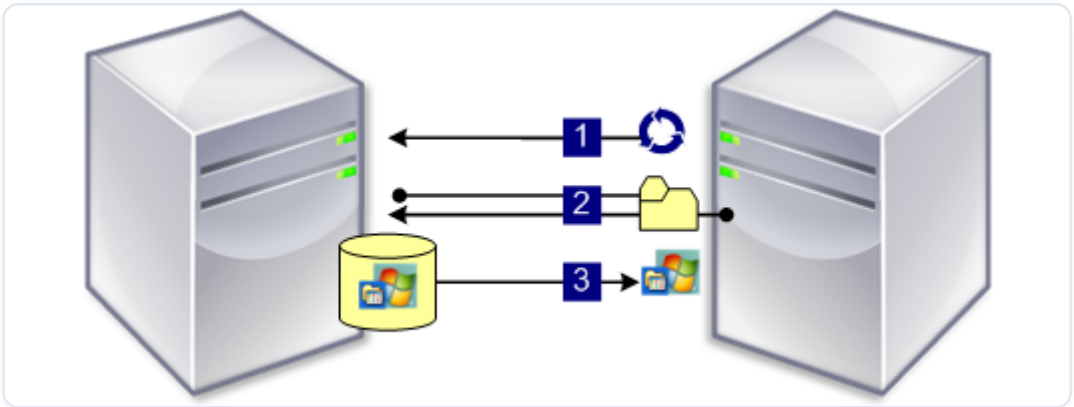
A virtual disk exists on any of the following locations:

- a Citrix Provisioning server
- a file share
- a storage system that communicates with the provisioning server using iSCSI, SAN, NAS, or CIFS connectivity

vDisks can be assigned to a single target device in private image mode, or to multiple target devices as standard image mode.

When a target device is turned on, it is set to boot from the network and to communicate with a provisioning server. The following occurs:

1. Processing takes place on the target device.
2. The target device downloads the boot file from a provisioning server and initiates the boot sequence.
3. Based on the device boot configuration settings, the appropriate virtual disk is located, then mounted on the provisioning server.



The software on that virtual disk is streamed to the target device as needed. To the target device, the virtual disk appears like a regular hard drive to the system.

Instead of immediately pulling all the virtual disk contents down to the target device, the data is brought across the network in real time, as needed. This approach allows a target device to get a new operating system and software in the time it takes to reboot, without requiring a visit to a workstation. This approach decreases the network bandwidth required by traditional disk imaging tools, which supports a larger number of target devices on your network without impacting overall network performance.

Components

This article provides an overview of Citrix Provisioning™ components.

License server

The license server is installed within the shared infrastructure or you can use an existing Citrix License Server. You select the license server when running the Configuration Wizard for the first time. All Citrix Provisioning servers within the farm must communicate with the license server.

Citrix Provisioning database

The database stores all system configuration settings that exist within a farm. Consider:

- Only one database can exist within a farm.
- All provisioning servers in that farm must be able to communicate with that database.
- Choose to use an existing SQL Server database or install SQL Server Express, which is free and available from Microsoft.

> **Note:**
>
> The database server is selected when the Configuration Wizard is run on a Citrix Provisioning server.

Citrix Provisioning console

The Citrix Provisioning console is a utility that is used to manage your Citrix Provisioning implementation. After logging on to the console, you select the farm that you want to connect to. Your administrative role determines what you can view in the console and manage in the farm.

Network services

Network services include a DHCP service, Preboot Execution Environment (PXE) service, and a TFTP service. These service options can be used during the boot process to retrieve IP addresses. These options can also be used to locate and download the boot program from the provisioning server to the target device. Alternative boot options are also available.

> **Tip:**

> Network services can be installed with the product installation and then configured using the Configuration Wizard.

Farms

A farm represents the top level of a Citrix Provisioning infrastructure. The farm is created when the Configuration Wizard is run on the first Citrix Provisioning server added to that farm.

All sites within a farm share that farm's Microsoft SQL database.

The console is not directly associated with the farm. Remote administration is supported on any console that can communicate with that farm's network.

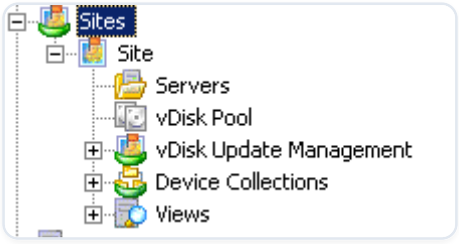
Stores

A farm contains one or more stores. A store is a logical name for a physical or virtual disk storage location. The store name is the common name used by all provisioning servers within the farm.

Sites

One or more sites can exist within a farm. The first site is created with the Configuration Wizard and is run on the first provisioning server in the farm.

Sites are represented in the console as follows:



Citrix Provisioning servers

A Citrix Provisioning server is any server that has Stream Services installed. The Stream Service is used to stream software from vDisks to target devices. In some implementations, vDisks reside directly on the provisioning server. In larger implementations, provisioning servers get the virtual disk from a shared-storage location on the network.

Provisioning servers also exchange configuration information with the Citrix Provisioning database. Provisioning server configuration options are available to ensure high availability and load balancing of target device connections.

Virtual disks

A virtual disk exists as disk image file on a provisioning server or on a shared storage device. A virtual disk consists of a .vhdx base image file, any associated properties files (.pvp), and if applicable, a chain of referenced VHD differencing disks (.avhdx).

Virtual disks are assigned to target devices. Target devices boot from and stream software from an assigned virtual disk image.

You may experience the following issues when implementing virtual disks in your environment:

- the virtual disk update schedule time cannot be applied after modifying it. It functions until you reboot the Citrix SOAP service.
- When importing VHDX files that you published from App Layering to the provisioned disk store, the operation may mistakenly report that you are using an invalid disk. You can eliminate this error by changing the period (.) characters in the published file name's date and time. A valid file name contains only one period for the .VHDX file extension.

Virtual disk pools

Virtual disk pools are the collection of all vDisks available to a site. There is only one virtual disk pool per site.

Virtual disk update management

The virtual disk Update Management feature is used to configure the automation of virtual disk updates using virtual machines. Automated virtual disk updates can occur on a scheduled basis, or can be invoked directly from the console. This feature supports updates detected and delivered from Electronic Software Delivery (ESD) servers, Windows updates, or other pushed updates.

Virtual disk modes

Virtual disk images are configured for **Private Image mode** or **Standard Image mode**. Consider the following when using virtual disk images:

- In Private Image mode, a virtual disk image is used as a single device supporting read/write characteristics.
- In standard image mode, a virtual disk image is used by multiple devices, but is read-only when using various caching options.

Virtual disk chain

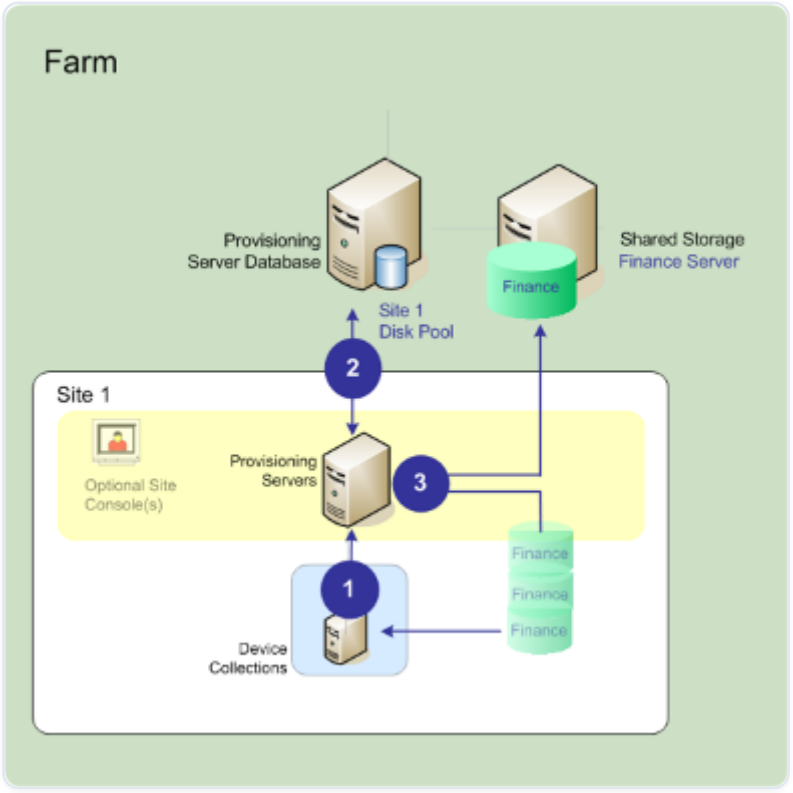
Any updates to a virtual disk base image can be captured in a versioned differencing disk, leaving the original base disk image unchanged.

Each time a virtual disk is updated, a new version of the VHDX differencing disk can be created. The file name is numerically incremented, as shown in the following table:

VIRTUAL DISK IMAGE	VHDX FILE NAME
Base Image	win7dev.avhdx
Version 1	win7dev.1.avhdx
Version 2	win7dev.2.avhdx
...	...
Version N	win7dev.**N**.avhdx

Booting from a virtual disk

The following image shows the method used to locate and boot from a virtual disk on a server share:



The preceding image illustrates the following steps:

1. The target device begins the boot process by communicating with a provisioning server and acquiring a license.
2. The provisioning server checks the virtual disk pool for virtual disk information, which includes identifying the servers providing the virtual disk to the target device. The server also verifies the path information used to get to the virtual disk. In this example, the virtual disk shows that only one provisioning server in this site can provide the target device with the virtual disk. The virtual disk physically resides on the Finance Server (shared storage at the farm level.
3. The provisioning server locates the virtual disk on Finance Server, then streams that virtual disk, on demand, to the target device.

Virtual disk examples

The following examples provide information about how Citrix Provisioning uses virtual disk images.

Example one

The physical virtual disk for Windows 10 resides on a Citrix Provisioning server local to a site. The logical name that is given to this physical location is the store.

Store name (logical name): bostonwin10

Physical path to the virtual disk is: C:\vDisks\

Example two

The physical virtual disk for Windows 10 resides on a network share (FinancevDisks) at the farm level.

Store name (logical name): FinancevDisks

Physical path to the virtual disk for all Provisioning Servers in the farm is: \financeserver\financevdisks\

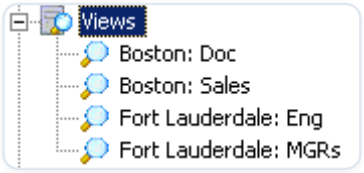
Device collections

Device collections are logical groups of target devices. A target device is a device, such as a desktop computer or a server, that boots and gets software from a virtual disk on the network. A device collection might represent a physical location, a subnet range, or a logical grouping of target devices. Creating device collections simplifies device management by enabling you to perform actions at the collection level rather than at the target-device level.

Views

Views allow you to quickly manage a group of target devices. Views are typically created according to business needs. For example, a view represents a physical location, such as a building, or a user type. A target device is a member of any number of views, although it is a member of only one device collection.

Views are represented in the console as follows:



Farm views can include any target device that exists in the farm. Site views include only target devices that exist within a site.

Product utilities

Citrix Provisioning™ includes several tools for configuring and managing deployment. After you have installed the software, the following tools become available:

- Installation Wizard – Use this wizard to install Citrix Provisioning components to create provisioning servers and master target devices.
- Configuration Wizard – Use this wizard to configure provisioning server components, including network services, and database permissions. This wizard is installed during the Citrix Provisioning installation process.
- Imaging Wizard – On the master target device, run the Citrix Provisioning Imaging Wizard. This process creates a virtual disk file in the database and then images that file without having to physically go to a Citrix Provisioning server. This utility is installed during the target device installation process.
- Virtual Disk Status Tray – Use this target device utility to get target-device connection status and streaming statistical information. This utility is installed during the Citrix Provisioning target device installation process.
- Citrix Virtual Apps and Desktops™ Setup Wizard – Creates virtual machines (VMs) on a Citrix Virtual Apps and Desktops hosted hypervisor server from an existing machine template. It creates and associates target devices to those VMs, assigns a virtual disk to each target device, then adds all virtual desktops to the catalog.

- Streamed VM Setup Wizard – Creates VMs on a hosted hypervisor from an existing machine template, creates, and associates target devices for each machine within a collection, then assigns a virtual disk image all the VMs.
- Virtual Host Connection Wizard – Adds new virtual host connections to the virtual disk Update Manager.
- Managed virtual disk Setup Wizard – Adds new managed vDisks to the virtual disk Update Manager.
- Update Task Wizard – Configures a new update task for use with virtual disk Update Manager.
- Boot Device Manager – Use this utility to configure a boot device, such as a USB or CD-ROM, which then receives the boot program from Citrix Provisioning.
- Upgrade Utilities – There are several upgrade methods available. The method you select depends on your network requirements.
- Programming Utilities – Citrix Provisioning provides programmers with a management application programming utility and a command line utility, accessed by all users. However, users can only use those commands associated with their administrator privileges. For example, a Device Operator is able to use this utility to get a list of all target devices that they have access to.

Administrator roles

The administrative role assigned to a user, or a group of users, controls the ability to view and manage objects within a Citrix Provisioning implementation. All members within a group share administrative privileges within a farm. An administrator has multiple roles if they belong to more than one group. Groups are managed at the farm level through the Console's Farm Properties window.

The following roles exist within a Citrix Provisioning™ farm:

- **Farm Administrator:** Farm administrators can view and manage all objects within a farm. Farm administrators can also create sites and manage role memberships throughout the entire farm.
- **Site Administrator:** Site administrators have full management access to the all objects within a site. For example, a site administrator can manage Citrix Provisioning servers, site properties, target devices, device collections, or virtual disk elements. A site administrator can also manage device administrator and device operator memberships.

- **Device Administrator:** Device administrators perform all device-collection management tasks on collections to which they have privileges. These tasks include viewing virtual disk properties (read-only) and assigning or removing virtual disks from a device. Tasks also include booting or shutting down target devices, editing device properties, and sending messages to target devices within a device collection to which they have privileges.
- **Device Operator:** Device operators view target device properties (read-only) and boot or shut down target devices. Also, device operators send messages to target devices within a device collection to which they have privileges.

Collections

Device collections allow you to create and manage logical groups of target devices. Creating device collections simplifies device management by performing actions at the collection level rather than at the target-device level.

> **Note:**
>
> A target device can only be a member of one device collection.

> A device collection represents a physical location, a subnet range, or a logical grouping of target devices. For example, a collection consists of all target devices that use a particular virtual disk image, and the collection might consist of maintenance, test, and production devices.

Alternatively, three device collections can exist for a particular virtual disk; one consisting of production devices, one consisting of test machines, and another consisting of maintenance machines. In the proceeding examples, all devices in a given collection are assigned to the same virtual disk.

Depending on a sites preference, another collection use case might include the consolidation of test and maintenance devices into a single device collection. This use case manages virtual disk assignments on a per device basis rather than a per collection basis. For example, create a device collection labeled *Development* consisting of five target devices, each one assigned to a particular virtual disk. Farm administrators create and manage device collections for sites they have security privileges to configure.

Expanding a **Device Collections** folder in the Console's tree allows you to view members of a device collection. To display or edit a device collection's properties, right-click on an existing device collection in the Console, then select the **Properties** menu option. The **Device Collection Properties** dialog displays. Use it to view or modify that collection.

You can perform actions on members of a device collection, such as rebooting all target devices members in this collection.

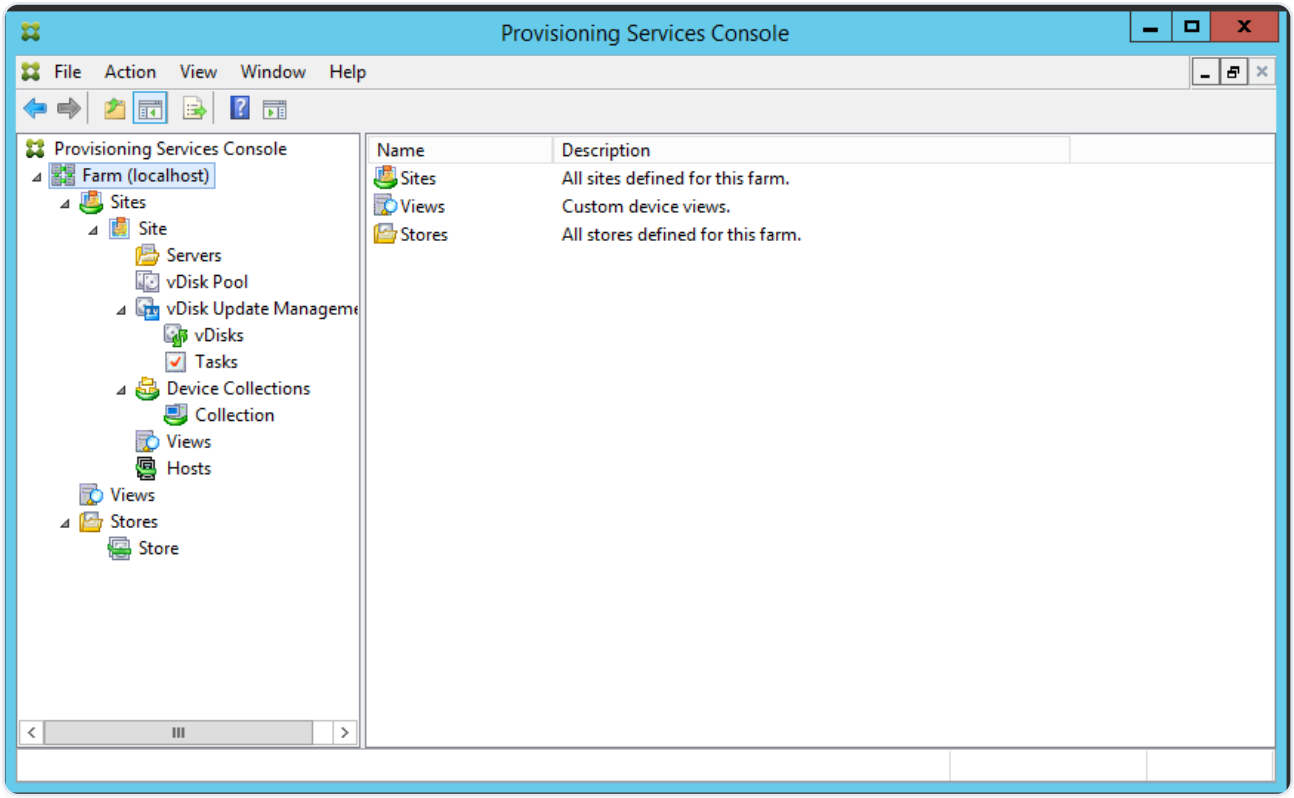
Citrix Provisioning™ console

Use the Citrix Provisioning console to manage components within a farm. The console can be installed on any machine that can access the farm. For more information about using the console to configure Citrix Provisioning, see the **Console** page.

> **Tip**
>
> To connect to a farm, see Farm Tasks.

Understanding the console window

In the console window, you can perform tasks when setting up, modifying, tracking, deleting, and defining the relationships among vDisks, target devices, and Citrix Provisioning servers.



Using the console tree

The tree is located in the left pane of the console window. It displays a hierarchical view of your network environment and managed objects within your network. The **Details view** display depends on the object you have selected in the tree and your user role.

In the tree, click **+** to expand a managed object node, or click **-** to collapse the node.

Basic tree hierarchy

Farm administrators can create sites, views, and stores within the farm. The farm level tree is organized as follows:

- Farm
  - Sites
  - Views
  - Stores

Site administrators generally manage those objects within sites to which they have privileges. Site's contain provisioning servers, a virtual disk pool, device collections, and views. The site level tree is organized as follows:

- Site
  - Servers
  - Device Collections
  - Virtual disk Pool
  - Virtual disk Update Management
  - Views

Using the details view

The right-hand pane of the console window contains the details view. This view provides information about the object selected in the tree, in table format. The types of objects that display in the view include provisioning servers, target devices, and vDisks. For more detailed information, right-click on the object, then select the **Properties** menu.

The tables that display in the details view can be sorted in ascending and descending order.

In the console, the objects that display and the tasks that you can perform depend on the assigned role.

Install Citrix Provisioning™ software components

Before installing Citrix Provisioning components, first understand the installation wizards that are described here. Then follow the installation and configuration procedures in the rest of the articles in this section.

> **Important:**
>
> Ensure that all Windows updates are current before installing Citrix Provisioning components. Sometimes, you need to install numerous updates. Citrix recommends that you reboot after installing all Windows updates. For Windows 10 1709, you must apply the OS update KB4093105, or later, before installing provisioning components.

> **Tip:**
>
> If you are using Linux streaming functionality, no new installation packages are provided at this release. Use the Provisioning Services 7.15 Linux DEB/RPM package. For example, after downloading the Citrix Provisioning 7.16 ISO, the target software for CentOS/Red Hat is pvs_RED_HAT_7.15_18089_x86_64.rpm.

Citrix® licensing

CTX_Licensing.msi installs the Citrix licensing software on a server that can communicate with provisioning servers within your implementation.

Citrix Provisioning installation wizard

Run PVS_Server.exe or PVS_Server_x64.exe to install the following Citrix Provisioning components within a farm:

- Citrix Provisioning Stream Service

- Network Boot Services (optional)
- Configuration Wizard (runs after the installation wizard to configure installed components and creates the Citrix Provisioning database)
- Programming Utilities
- Boot Device Manager (BDM)

> **Note:**
>
> Installing from a UNC path is not supported.

Citrix Provisioning console wizard

Run PVS_Console.exe or PVS_Console_x64.exe to install the Citrix Provisioning console, which also includes the Boot Device Management utility. The console can be installed on any machine that can communicate with the Citrix Provisioning database.

Master target device installation wizard

For Windows: PVS_Device.exe or PVS_Device_x64.exe

Installs the target device software on a master target device. The master target device is used to create the 'golden image,' which is then saved to a vDisk file using the Imaging Wizard.

Upgrade wizard

The Upgrade Wizard must be installed and run in a folder that does not contain surrogate pair characters. These characters represent the Unicode code point after 0x10000. The Upgrade Wizard facilitates the automation of the upgrade process, and includes the following utilities:

- The UpgradeAgent.exe, which runs on the target device to upgrade previously installed product software.
- The UpgradeManager.exe, which runs on the provisioning server to control the upgrade process on the target device.

Uninstall

Removing the software from your system requires that you uninstall both the provisioning server and target device components.

Uninstalling Citrix Provisioning

1. On the provisioning server, open the system's **Control Panel**. From the **Windows Start** menu, select **Settings**, and then click **Control Panel**.
2. Double-click on the **Programs and Features** icon.
3. Select **Citrix Provisioning**, then click the **Uninstall** menu option.

Uninstalling Windows target device software

1. Set the system BIOS to boot from the original hard drive.
2. Reboot the target device directly from the hard drive.
3. On the target device, open the system’s **Control Panel**.
4. Double-click on the **Programs and Features** icon.
5. Select the **Citrix Provisioning**, then click the **Uninstall** menu option.

Uninstalling the Citrix Provisioning console

1. On a machine in which the console is installed, open the system's **Control Panel**.
2. Double-click the **Programs and Features** icon.
3. Select the **Citrix Provisioning**, then click the **Uninstall** menu option.

Uninstalling components that use Windows 10 Creator

Citrix Provisioning cannot be uninstalled using the **App and Feature** screen in Windows 10 Creator. This issue occurs in all MSI installers.

To uninstall target or console provisioning software:

1. Access the Citrix Provisioning component you want to remove in the **Windows Start** menu. Right-click to expose a contextual menu.
2. In the contextual menu, click **Uninstall**. The **Program and Features** screen appears.
3. In the **Program and Features** screen, select the components you want to remove.

Pre-installation tasks

Complete the following tasks before installing and configuring Citrix Provisioning.

> **Important:**
>
> Ensure all Windows updates are current before installing Citrix Provisioning components. Citrix recommends that you reboot after installing all Windows updates.

Select and configure the Microsoft SQL database

Each Citrix Provisioning farm has a single database. You can provide the database on either:

- An existing SQL Server or SQL Server Express instance
- A new server running SQL Server or SQL Server Express
- A new or existing Azure SQL Database instance

All Citrix Provisioning servers in a farm must be able to communicate with the database server.

In a production environment, to avoid poor distribution during load balancing, best practice is to install the SQL Server or SQL Server Express instance and the Citrix Provisioning server component software on separate servers.

There are three ways to create the database:

- Use the Configuration wizard. To use this option, you need `dbcreator` permission.
- If you do not have permission to create databases, use the **DbScript.exe** utility to create a SQL script that a database administrator can run to create the provisioning database. This utility is installed with the provisioning software.
- If the database administrator creates an empty database by running the DbScript.exe utility, then this database is chosen as the database for the new farm when running the Configuration wizard. The login used when running the Configuration wizard must be the owner of the database. Also, this login must have the **View any definition** permission. The database administrator sets this permission when the empty database is created.

Run the DbScript.exe utility to create or update the database

If you do not have permission to create databases, use **DbScript.exe** to generate a SQL script for the database administrator to run to create or update the Citrix Provisioning database. Run the

script from the Windows command prompt in `C:\Program Files\Citrix\Provisioning Services`.

To generate the script to create the database, use this syntax:

- For SQL Server and SQL Server Express: `DbScript.exe -new <databaseName> <farmName> <siteName> <collectionName> <farmAdminGroup> <adGroupsEnabled> <scriptName> <is2012orHigher>`
- For Azure SQL Database: `DbScript.exe -newForAzSqlDb <databaseName> <farmName> <siteName> <collectionName> <farmAdminGroup> <adGroupsEnabled> <scriptName> <is2012orHigher>`

When creating a new database for Azure SQL Database, DbScript produces two script files instead of one.

- The first is run into the master database, and it creates the new database.
- The second script is then run into the new database.

To generate the script to update the database, enter:

```
DbScript.exe -upgrade <databaseName> <scriptName>
```

The commands use these arguments:

- `<databaseName>` — Name of the database to update.
- `<farmName>` — Farm name for the database.
- `<siteName>` — Site name for the database.
- `<collectionName>` — Collection name for the database
- `<farmAdminGroup>` — Farm administrator group, specified as a full path.

  > **Note:**
  >
  > When you run the Configuration wizard, you must be a member of this group (an Active Directory group) to add the Citrix Provisioning servers to the database.

- `<adGroupsEnabled>` — Enable or disable AD groups, specified as Boolean, where `true` enables AD groups and `false` disables AD groups.
- `<scriptName>` — Name of the script to generate, specified as a full path.

- `<is2012orHigher>` — This is deprecated. Use `true`.

DbScript.exe examples

This example generates a script to create an empty Citrix Provisioning database called `db1-2`. The script is called **newDb.sql** and is located in `C:`.

```
C:\Program Files\Citrix\Provisioning Services> DbScript.exe -new db1-2 Farm1 Site1 Collection1 "test.local/Users/Domain Users" true c:\newDb.sql true
```

This example generates a script to upgrade the Citrix Provisioning database `test1`. The script is called **upgrade.sql** and, because no path is specified, is located in the directory where the script was run (`C:\Program Files\Citrix\Provisioning Services`).

```
C:\Program Files\Citrix\Provisioning Services>DbScript.exe -upgrade test1 upgrade.sql
```

Database sizing

For information, see database sizing.

When the database is created, its initial size is 20 MB with a growth size of 10 MB. The database log initial size is 10 MB with a growth size of 10%.

The base amount of space required is 112 KB, which does not change. The base image includes the following:

- DatabaseVersion record requires approximately 32 KB
- Farm record requires approximately 8 KB
- DiskCreate record requires approximately 16 KB
- Notifications require approximately 40 KB
- ServerMapped record requires approximately 16 KB

The variable amount of space required, based on objects, is as follows:

- Access and groupings (each)
  - A User group that has access to the system requires approximately 50 KB
  - A Site record requires approximately 4 KB
  - A Collection requires approximately 10 KB
- FarmView (each)

  - FarmView requires approximately 4 KB
  - FarmView/Device relationship requires approximately 5 KB
- SiteView (each)
  - SiteView requires approximately 4 KB
  - SiteView/Device relationship requires approximately 5 KB
- Target device (each)
  - A target device requires approximately 2 KB
  - `DeviceBootstrap` requires approximately 10 KB
  - `Device:Disk` relationship requires approximately 35 KB
  - `DevicePersonality` requires approximately 1 KB
  - `DeviceStatus` when a Device boot requires approximately 1 KB
  - `DeviceCustomProperty` requires approximately 2 KB
- Disk (each)
  - Unique disk requires approximately 1 KB
  - `DiskVersion` requires approximately 3 KB
  - `DiskLocator` requires approximately 10 KB
  - `DiskLocatorCustomProperty` requires approximately 2 KB
- Provisioning server (each)
  - A server requires approximately 5 KB
  - `ServerIP` requires approximately 2 KB
  - `ServerStatus` when a Server boot requires approximately 1 KB
  - `ServerCustomProperty` requires approximately 2 KB
- Store (each)
  - Store requires approximately 8 KB
  - Store:Server relationship requires approximately 4 KB
- Disk update (each)
  - `VirtualHostingPool` requires approximately 4 KB

- `UpdateTask` requires approximately 10 KB
- `DiskUpdateDevice` requires approximately 2 KB
- Each `DiskUpdateDevice:Disk` relationship requires approximately 35 KB
- `Disk:UpdateTask` relationship requires approximately 1 KB

The following changes cause the size requirements to increase:

- Each processed task (for example: Virtual disk versionings merge) requires approximately 2 KB.
- If auditing is turned on, each change made by the administrator in the Citrix Provisioning console, MCLI, or PowerShell interface requires approximately 1 KB.

Database mirroring

For Citrix Provisioning to support MS SQL database mirroring, the database needs to be configured with **High-safety mode with a witness (synchronous)**.

For information on how to configure and use database mirroring, see Database mirroring.

Implement database clustering

To implement database clustering:

1. Follow Microsoft's instructions.
2. Run the Citrix Provisioning Configuration wizard.
3. Specify the **Availability Group listener** as the database server. No instance is used.
4. Enable **Multi-Subnet Failover** in the Connection Options.

Supported authentication types

The table helps you determine how you want Citrix Provisioning to authenticate with the database, and the credentials you want to use when authenticating.

AUTHENTICATION TYPE	GRANTS ACCESS TO	REQUIRED CREDENTIALS	DATABASE PLATFORM	OTHER RESTRICTIONS
Active Directory Integrated	Active Directory User. Create the username in Active	Nothing (uses the current login context)	SQL Server	The Citrix Provisioning server must belong to a

AUTHENTICATION TYPE	GRANTS ACCESS TO	REQUIRED CREDENTIALS	DATABASE PLATFORM	OTHER RESTRICTIONS
	Directory if you do not want to use an existing one.			domain, the Citrix Provisioning Service user context must be a domain user, and a domain user must configure Citrix Provisioning.
SQL Server	SQL Login. Create the SQL login on the database server if you do not want to use an existing one.	Login and Password	SQL Server and Azure SQL Database	

Note:

For information on supported authentication types for Citrix Provisioning on Azure, see Supported authentication types in Citrix Provisioning on Azure article.

Configure authentication

Citrix Provisioning can use **Active Directory Integrated** authentication or **SQL Server** authentication to access the database.

Configuration wizard user permissions

You must have the system privilege of a local administrator to run the configuration wizard.

The **admin database principal** is the database principal used by the configuration wizard to create and set up the provisioning database. The authentication credentials that you specify in the configuration wizard identify the database principal.

- If you choose **Active Directory Integrated** authentication, the configuration wizard accesses the database as the user running the configuration wizard (an Active Directory user).
- If you choose **SQL Server** authentication, then the configuration wizard accesses the database as a different principal.

See Supported authentication types for more information on selecting an admin database principal.

> **Note:**
>
> The database admin principal is only used while running the configuration wizard. It is not saved and not used by the Stream and SOAP services. You must use a principal with elevated privileges for Stream and SOAP services.

- When using SQL Server, the admin database principal requires the following permissions:
  - `securityadmin` for creating and updating server logins (when using SQL Server)
  - `db_owner` for any existing database

To create a database for a new farm, the admin database principal requires `dbcreator` as an additional permission. See Select and configure the Microsoft SQL database for information on different ways to create the database.

- When using Azure SQL Database, the admin database principal requires the following permissions:
  - `loginmanager` for creating and updating server logins
  - `db_owner` for any existing database

  To create a database for a new farm, the admin database principal requires `dbmanager` as an additional permission.

  `loginmanager` and `dbmanager` are special user roles that are assigned to users in the master database.

Service account permissions

The service account for the Stream and SOAP services must have the following system privileges:

- Run as service
- Registry read access

- Access to `Program Files\Citrix\Citrix Provisioning`
- Read and write access to any virtual disk location.

The **service database principal** is the database principal used by the services to access the provisioning database. The authentication credentials that you specify in the configuration wizard identify the database principal.

- If you choose **Active Directory Integrated** authentication, the services access the database as the service account (an Active Directory user).
- If you choose **SQL Server** authentication, then the services can access the database as a different principal.

See Supported authentication types for more information on selecting a service database principal.

The configuration wizard configures the database to ensure that the service database principal has the following permissions:

- `db_datareader`
- `db_datawriter`
- Run permissions on stored procedures

Determine which of the following supported user accounts the Stream and SOAP services run under:

- Network service account

  Minimum privilege local account, which authenticates on the network as a computers domain machine account
- Specified user account (required when using a Windows Share), which can be a Workgroup or domain user account

Support for KMS licensing requires the SOAP Server user account to be a member of the local administrators group.

> **Tip:**
>
> Authentication is not common in workgroup environments, as a result, minimum privilege user accounts must be created on each server and each instance must have identical credentials.

> Determine the appropriate security option to use in this farm. Only one option can be selected per farm and the selection you choose impacts role-based administration. For security options:

- Use Active Directory groups for security (default); select this option if you are on a Windows **Domain running Active Directory**. This option enables you to use Active Directory for Citrix Provisioning administration roles.

  > **Note:**
  >
  > Windows 2000 Domains are not supported.

- Use Windows groups for security. Select this option if you are on a single server or in a Workgroup. This option enables you to use the Local User/Groups on that particular server for Citrix Provisioning administration roles.

Console users do not directly access the database.

Minimum permissions required for more provisioning functionality include:

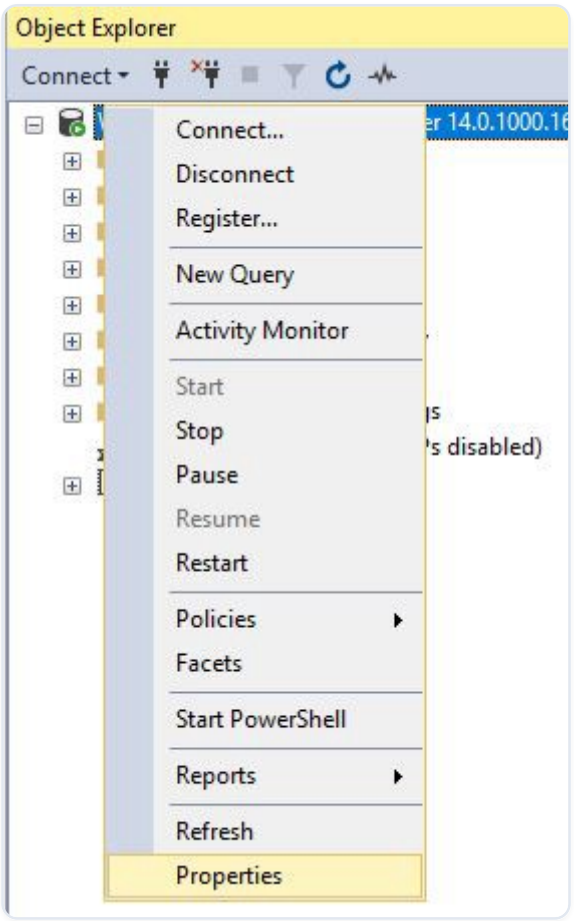
- Citrix Virtual Apps and Desktops™ Setup wizard, Streamed VM Setup wizard, and ImageUpdate service
  - vCenter, SCVMM, and XenServer (formerly Citrix Hypervisor™) minimum permissions
  - Permissions for the current user on an existing Citrix Virtual Apps™ and Desktops controller
  - A Citrix Provisioning console user account configured as a Citrix Virtual Apps and Desktops administrator added to a provisioning `SiteAdmin` group or higher
  - Active Directory Create Accounts permission to create accounts in the console. To use existing accounts, Active Directory accounts have to exist in a known OU for selection
- AD account synchronization: create, reset, and delete permissions
- Virtual disk: Privileges to perform volume maintenance tasks

> **Note:**
>
> A service account does not require special AD permissions.

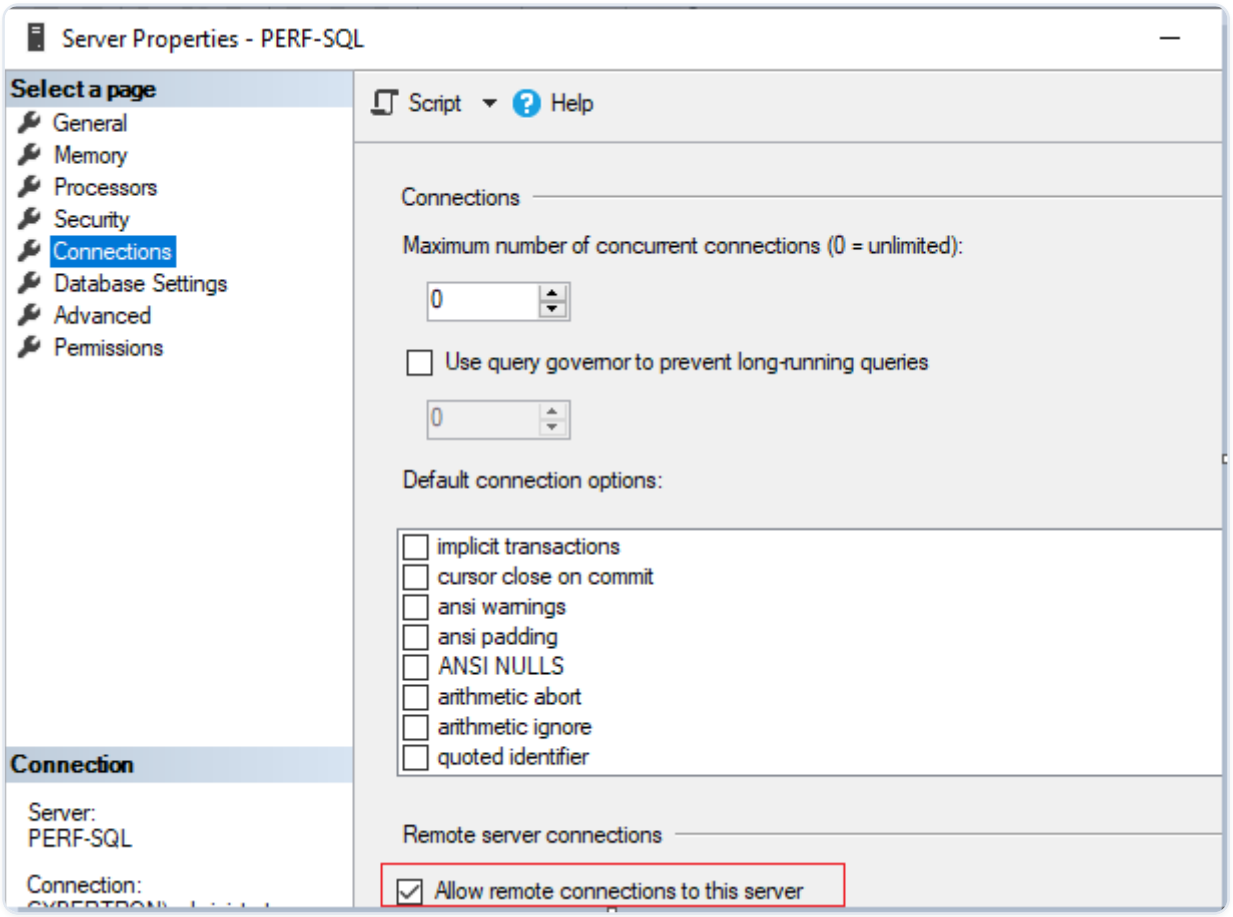
Enable a remote connection in SQL Server

Use the information in this section to establish a remote connection to the SQL server.

1. Log into the SQL server using **SQL Server Management Studio**.
2. In the object explorer window, right-click the SQL server and choose **Properties**:

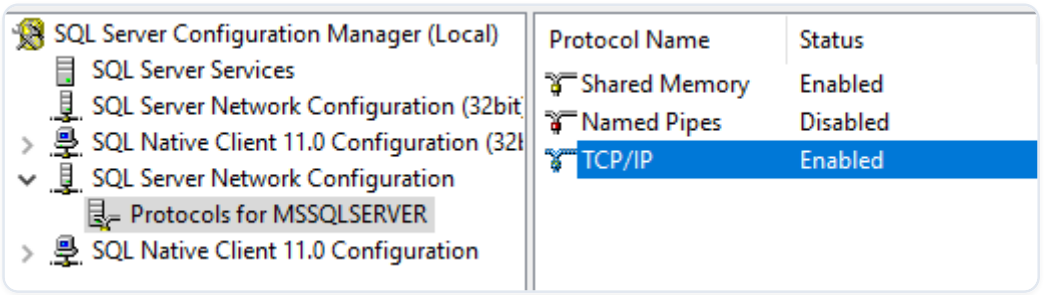


3. In the **Object Explorer** window, select the **Connections** node. Under **Remote server connections**, select or clear the **Allow remote connections to this server** check box:



After updating the remote server connection:

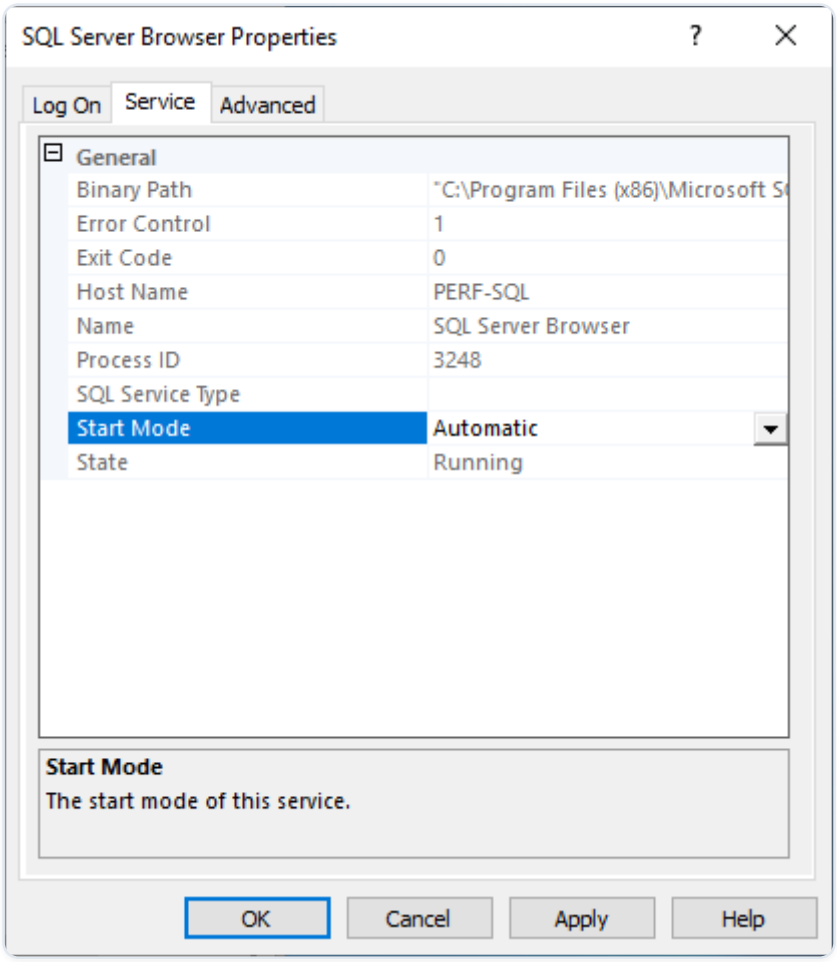
1. In the **Start** menu, click **Start > Microsoft SQL Server *version* > SQL Server *version* Configuration Manager**. The **SQL Server Configuration Manager** window appears.
2. Expand the option **SQL Server Network Configuration**. Select **Protocols for (your server name)**. Select **TCP/IP** and right click. In the contextual menu, choose **Enable**. Click **OK** to restart the service.



After restarting the service, change the **Start mode**. In the **SQL Server Configuration Manager** window:

1. Select **SQL Server Services**. In the right pane, right-click the **SQL Server Browser** option to expose a contextual menu.
2. Choose **Properties**.
3. In the **Service** tab, change the **Start Mode** to **Automatic**.

4. Click **OK**.

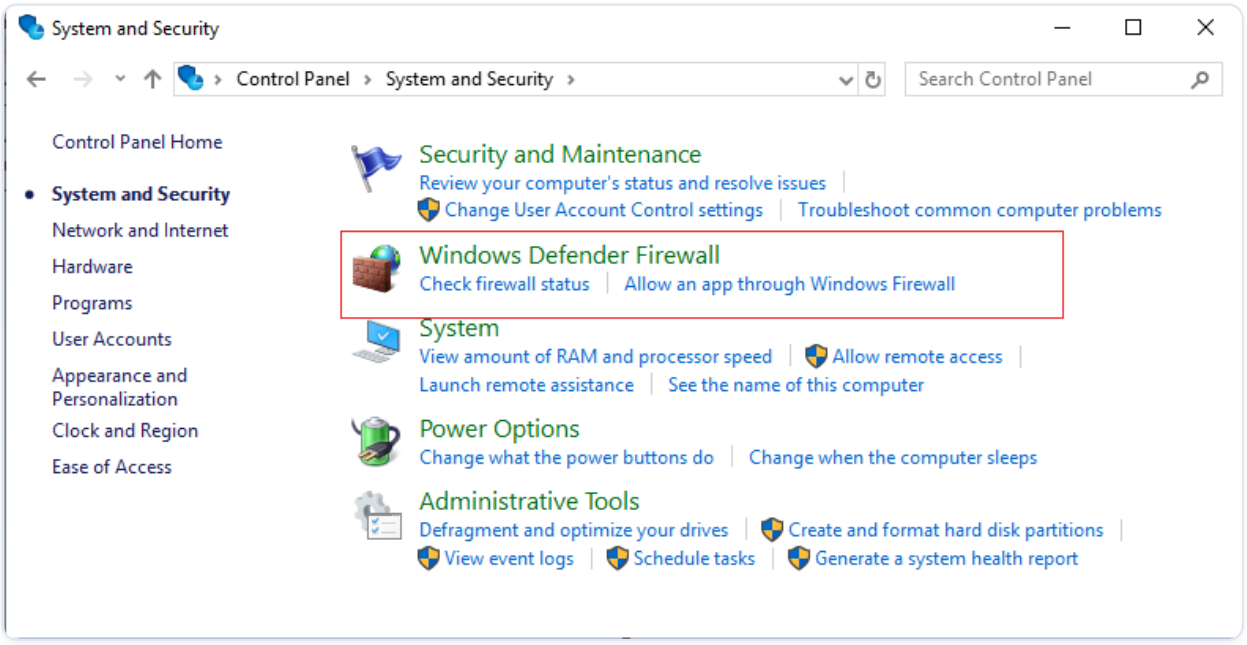


1. Select the **SQL Server Browser** and right-click to open a contextual menu. Click **Start**.
2. Select the SQL Server service that corresponds to the instance and right-click to open a contextual menu. Click **Restart**.

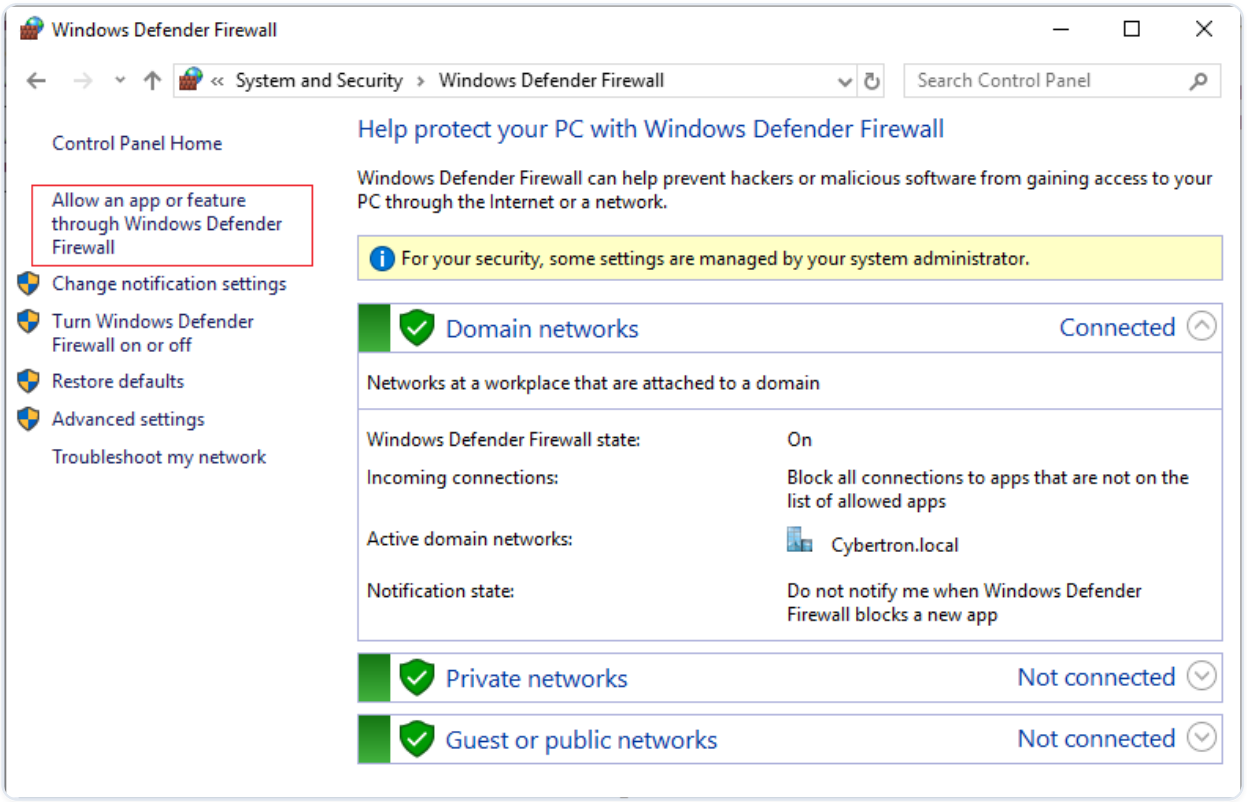
Create an exception for SQL Server in Windows Firewall

Use the information in this section to create an exception for SQL Server in environments using the Windows Firewall:

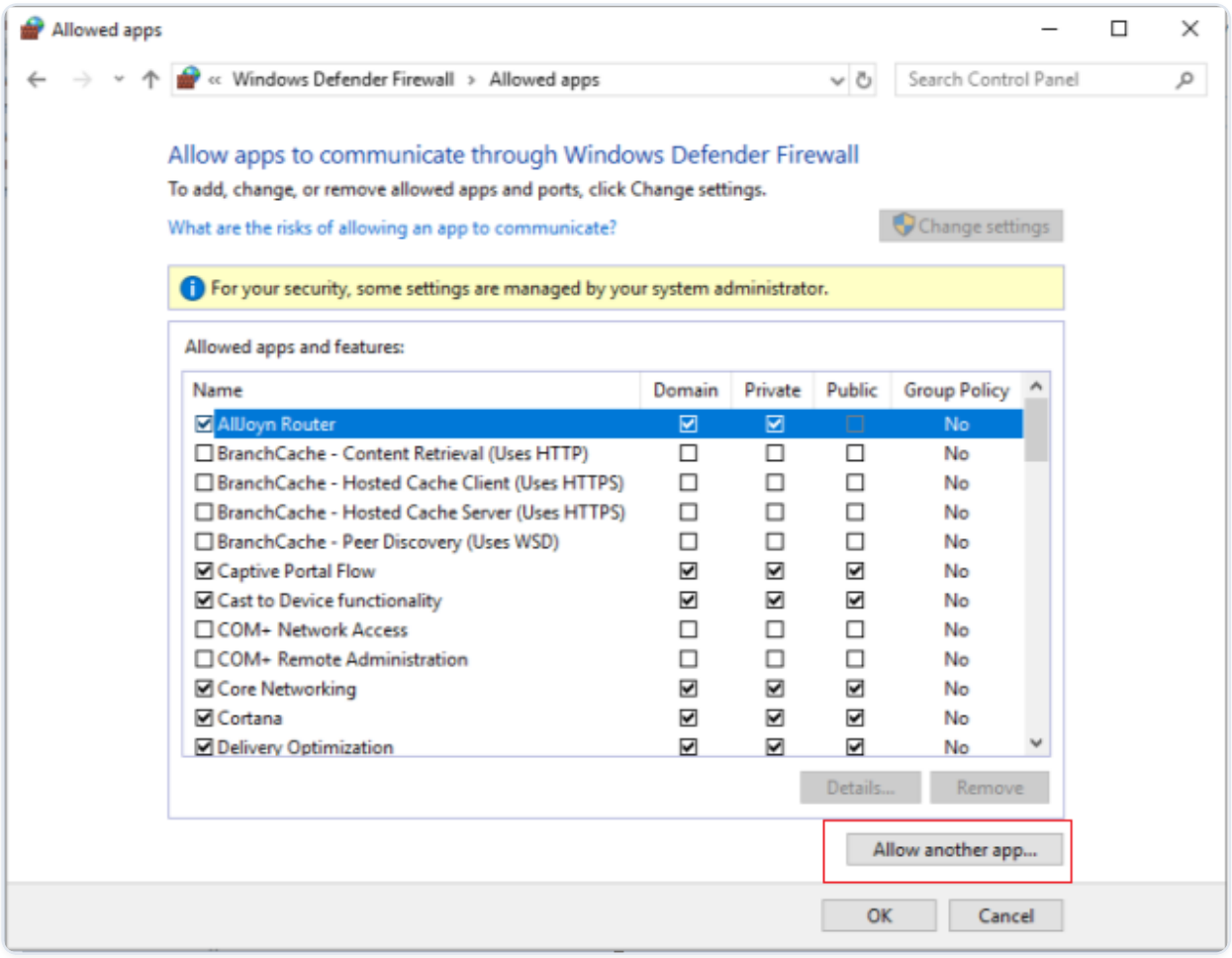
1. Open the **Control panel** and select **System and Security**.
2. Select **Windows Defender Firewall**:



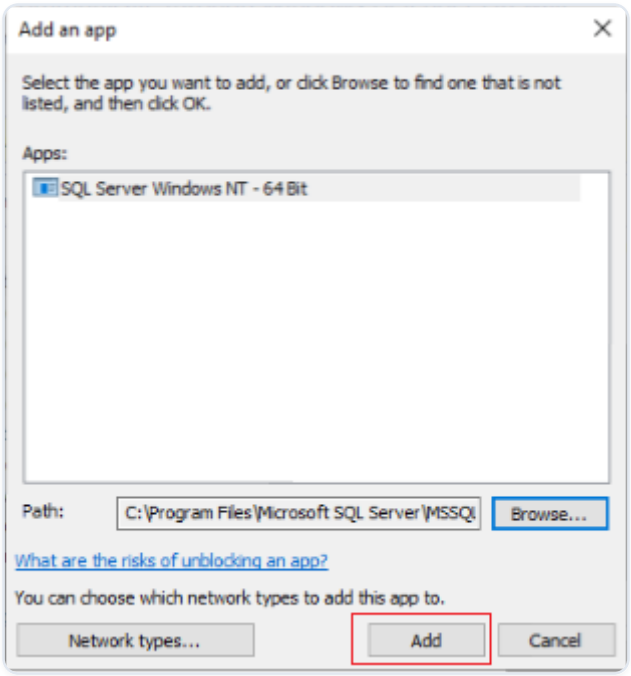
3. Click **Allow an app or feature through Windows Defender Firewall**. Turn on Windows Firewall:



4. In the **Allow apps to communicate through Windows Defender Firewall** window, click **Allow another app…**:



5. In the **Add an app** screen, click **Browse**.
6. Browse to the SQL Service `sqlserver.exe` and click **Open**. The default path to `sqlserver.exe` is:
   - SQL 2019 – `C:\Program Files\Microsoft SQL Server\MSSQL15.<SQL Instance Name>\MSSQL\Binn`
   - SQL 2017 – `C:\Program Files\Microsoft SQL Server\MSSQL14.<SQL Instance Name>\MSSQL\Binn`
7. Click **Add**:



1. Repeat steps 4–7 for `C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe`.
2. Click **OK**.

Enable secure connection from provisioning server to SQL server

SQL server, license server, and provisioning server can be configured to enable secure connection.

Use the information in this section to establish a secure connection to the SQL server.

On the SQL server computer:

1. Obtain a server certificate with a private key that can be used as the SQL server's server certificate. You can obtain the server certificate from a trusted authority or use a self-signed certificate. The server certificate and private key should be in a `.PFX` file. The common name must be the FQDN of the SQL server computer.
2. Import the certificate and the key in the personal certificates folder of the local computer certificate store on the SQL server computer.
3. Give the SQL server access to the certificate and key.
4. Do the following to configure the SQL server to force secure connections.
    a. Run the **SQL Server Configuration Manager**.
    b. From the left pane, select **SQL Server Network Configuration > Protocols for instance**.
    c. Right-click to select **Properties**.
    d. In the **Flags** tab, set **Force Encryption** to **Yes**.

e. In the **Certificate** tab, select the server certificate from the drop-down list. If this certificate is not in the list, then verify that it was imported as described.

f. Click **OK** and restart the SQL server service for the instance.

On the Citrix Provisioning server computer:

1. Deploy the necessary certificate authority certificates that are required to trust the server certificate.

    a. If the authority is not trusted:

        i. Obtain the authority certificate.

        ii. Import that certificate into the Trusted Root Certificate Authorities folder of the local computer certificate store.

    b. If the server certificate is self-signed:

        i. On the SQL server computer, export the certificate only into a certificate file.

        ii. Copy this certificate to the Citrix Provisioning server computer.

        iii. Import this certificate into the Trusted Root Certificate Authorities folder of the local computer certificate store.

2. Configure the provisioning server to connect to the SQL server using the same name as in the certificate, which is the FQDN of the SQL server computer. If necessary, run the Configuration Wizard, and join the Farm again. Using this method, you can change the database server name.

Kerberos security

By default, the Citrix Provisioning console, Imaging wizard, PowerShell snap-in, and MCLI use Kerberos authentication when communicating with the SOAP Service in an Active Directory environment. Part of the Kerberos architecture is for a service to register (create a service principal name, SPN) with the domain controller (Kerberos Key Distribution Center). The registration is essential because it allows Active Directory to identify the account that the SOAP service is running in. If the registration is not performed, the Kerberos authentication fails and Citrix Provisioning falls back to using NTLM authentication.

The Citrix Provisioning SOAP Service registers every time the service starts and unregisters when the service stops. However, the registration fails if the service user account does not have

permission. By default, the Network Service account and domain administrators have permission while normal domain user accounts do not.

To work around this permissions issue, do either of the following:

- Use a different account that has permissions to create SPNs.
- Assign permissions to the service account.

ACCOUNT TYPE	PERMISSION
Computer Account	Write Validated SPN
User Account	Write Public Information

Network components

This article describes the tasks necessary to carry out to manage the network components within your streaming implementation.

Preparing network switches

Network switches provide more bandwidth to each target device and are common in networks with large groups of users. The use of Citrix Provisioning™ in the network might require changes to switch configurations. When planning an implementation, give special consideration to managed switches.

> **Note:**
>
> For Citrix Provisioning networks, you must specify all network switch ports to which target devices are connected as edge-ports.

> Managed switches usually offer loop detection software. This software turns off a port until the switch is certain the new connection does not create a loop in the network. While important and useful, the delay prevents your target devices from successfully performing a PXE boot.

This problem manifests itself in one of the following ways:

- Target device (not Windows) login fails.

- Target device appears to hang during the boot process.
- Target device appears to hang during the shutdown process.

To avoid this problem, you must disable the loop detection function on the ports to which your target devices are connected. Specify all ports to which target devices are connected as edge-ports. Specifying all ports has the same effect as enabling the fast link feature in older switches (disables loop detection).

> **Note:**
>
> A network speed of at least 100 MB is highly recommended. If using a 10 MB hub, check whether your network card allows you to clear auto-negotiation. Turning auto-negotiation off can resolve potential connection problems.

Switch manufacturers

This feature is given different names by different switch manufacturers. For example:

- Cisco; PortFast, Spanning Tree Protocol (STP) Fast Link, or switch port mode access
- Dell; STP Fast Link
- Foundry; Fast Port
- 3COM; Fast Start

Using Uniform Naming Convention (UNC) names

A Universal Naming Convention (UNC) format name defines the location of files and other resources that exist on a network. UNC provides a format so that each shared resource can be identified with a unique address. Windows and many network operating systems (NOSs) support UNC.

With Citrix Provisioning, UNC format names can be used to specify the location of the OS Streaming database for all provisioning servers. UNC format also specifies the location of a particular virtual disk.

Syntax

UNC names conform to the `\SERVERNAME\SHARENAME` syntax, where `SERVERNAME` is the name of the provisioning server and `SHARENAME` is the name of the shared resource.

UNC names of directories or files can also include the directory path under the share name, with the following syntax:

```
\SERVERNAME\SHARENAME\DIRECTORY\FILENAME
```

For example, to define the folder that contains your configuration database file in the following directory:

```
C:\Program Files\Citrix\Provisioning Services
```

On the shared provisioning server (server1), enter:

```
\server1\Citrix Provisioning
```

> **Note:**
>
> UNC names do not require that a resource is a network share. UNC can also be used to specify local storage for use by only a local machine.

Accessing a remote network share

To access a remote network share using a UNC format name, the Stream Service must have a user account name and password on the remote system.

To use a UNC name to access a remote network share:

1. On the provisioning server, create a user account under which the stream service runs. This account must have a password assigned, otherwise the stream service fails to log in correctly. Your stream service shares the user account and password, or separate user accounts and passwords can be set up for each service.
2. Share the virtual disk and configuration database folders. In Windows Explorer, right-click on the folder, then select **Properties**. Click the **Sharing** tab, then select the **Share this** folder radio button. Enter or select a share name.
3. Make sure permissions are set to allow full control of all files in the virtual disk folder and database folder. Click the **Permissions** button on the **Sharing** tab, or click the **Security** tab, then set the correct permissions.
4. For the Stream Service:

- Go to **Control Panel > Computer Management > Component Services**, right-click the **Stream Service**, and select **Properties**.
- Click the **Log On** tab. Change the Logon to: setting to **This Account**, and set up the service to log in to the user and password configured in Step 1.

5. Verify that all Stream Services are restarted. The Configuration Wizard performs this step automatically. Stream services can also be started from the console or from the **Control** Panel.

> **Note:**
>
> Do not use a mapped drive letter to represent the virtual disk or database location directories when configuring Stream Services. The Stream service cannot access folders using a mapped drive letter for the directory because the mapped drives did not exist when the services started at boot time.

Reducing network utilization

Windows provides several features that presume the use of a large, fast hard-disk. While many of these features are useful on a diskless system where the disk is on the network, using them decreases cache effectiveness and increases network utilization. In environments that are sensitive to network utilization, consider reducing the effect of these features by disabling them or adjusting their properties.

In particular, offline folders are not useful on a diskless system and can be detrimental to the performance of Windows on a diskless system. Offline folders cache network files — a feature that is not applicable to a system where all files are on the network.

All of these features are configurable through the target device itself. The following features are configurable in the Windows **Group Policy**.

- Offline Folders
- Event Logs

Configure Windows features on a standard virtual disk

1. Prepare a Standard Image virtual disk for configuration.
    - Shut down all target devices that use the Standard Image virtual disk.
    - In the Citrix Provisioning console, change the **Disk Access Mode** to **Private Image**.

- Boot one target device.

2. Configure one or more features.
3. Prepare the Standard Image virtual disk for use
    - Shut down the target device previously used to configure the virtual disk.
    - From the Console, change the Disk Access Mode to Standard Image.
    - Boot one or more target devices.

Configure the recycle bin

If you disable the recycle bin, files are deleted immediately. Therefore, the file system reuses respective disk sectors and cache entries sooner.

To configure the recycle bin:

1. From the target device, or Windows Explorer, right-click the **Recycle Bin**.
2. Select **Properties**.
3. Select **Global**.
4. Select from the following settings:
    - Use one setting for all drives
    - Do not move files to the Recycle Bin. Remove files immediately when deleted.

Configure offline folders

Disabling offline folders is recommended to prevent Windows from caching network files on its local disk – a feature with no benefit to a diskless system. Configure this feature from the target device or using Windows Group Policy.

To configure from the target device:

1. Open **Windows Explorer**.
2. Select **Tools > Folder Options**.
3. Select **Offline Folders**.
4. Clear **Enable Offline Folders**.

To configure using the Windows **Group Policy**:

On the domain controller, use the Microsoft Management Console with the Group Policy snap-in to configure the domain policies for: administration templates, network, or offline files. Policy setting objects include:

- Policy setting object: Disable user configuration of offline files (Enabled).
- Policy setting object: Synchronize all offline files before logging off (Disabled).
- Policy setting object: Prevent use of the **Offline Files** folder (Enabled).

Configure event logs

Reduce the maximum size of the Application, Security, and System Logs. Configure this feature using the target device or Windows Group Policy.

To configure event logs, on the target device:

1. Select **Start > Settings > Control Panel**.
2. Open **Administrative Tools > Event Viewer**.
3. Open the properties for each log.
4. Set the Maximum log size to a relatively low value. Consider 512 kilobytes.

To configure using the Windows **Group Policy**:

On the domain controller, use the Microsoft Management Console with the Group Policy snap-in to configure the domain policies for the following object:

- Policy setting: Policy Maximum Application Log Size. Relatively low value. Consider 512 kilobytes.
- Policy setting: Policy Maximum Application Log Size. Relatively low value. Consider 512 kilobytes.
- Policy setting: Policy Maximum Application Log Size. Relatively low value. Consider 512 kilobytes.

Disable Windows automatic updates

If you have the Windows automatic updates service running on your target device, Windows periodically checks a Microsoft website and looks for security patches and system updates. Uninstalled updates are downloaded and installed automatically. Normally, an automatic update is a useful feature for keeping your system up-to-date. However, in a Citrix Provisioning implementation using standard image mode, this feature can decrease performance, or even cause more severe problems. Performance degradations occur because the Windows automatic

updates service downloads programs that fill the write cache. When using the target device's RAM cache, filling the write cache can cause your target devices to stop responding.

Rebooting the target device clears both the target device and Citrix Provisioning write cache. Rebooting after an auto-update means that the automatic update changes are lost, which defeats the purpose of running automatic updates.

> **Tip:**
>
> To make Windows updates permanent, apply them to a virtual disk while it is in Private Image mode.
>
> To prevent filling your write cache, disable the Windows Automatic Updates service for the target device used to build the virtual disk.

To disable the Windows automatic updates feature:

1. Select **Start > Settings > Control Panel > Administrative Tools**.
2. Select **System**.
3. Click the **Automatic Updates** tab.
4. Select the **Turn Off Automatic Updates radio** button.
5. Click **Apply**.
6. Click **OK**.
7. Select **Services**.
8. Double-click the **Automatic Updates** service.
9. Change the **Startup Type** by selecting **Disabled** from the menu.
10. If the Automatic Updates service is running, click **Stop** to stop the service.
11. Click **OK** to save your changes.

To make Windows updates permanent:

1. Shut down all target devices that share the virtual disk.
2. Change the virtual disk mode to **Private image**.
3. Boot one target device from that virtual disk.
4. Apply Windows updates.

5. Shut down the target device.
6. Change virtual disk mode to **Standard image**.
7. Boot all target devices that share this virtual disk.

Managing roaming user profiles

A Roaming User Profile is a user profile that resides on a network share. It consists of files and folders containing the user's personal settings and documents. When a user logs on to a target device system in the domain, Windows copies the respective profile from a network share to the target device's disk. When logging off, Windows synchronizes the user profile on the target device's hard disk with the user profile on the network share.

For a diskless target device, its disk is actually a virtual disk residing in shared storage. Therefore, the profile returns back to the shared storage containing the virtual disk. Since the persistent user data always resides on shared storage, Windows does not need to download the profile, saving time, network bandwidth, and file cache. Since some of the files included in the profile can grow large, the savings can be significant.

Using Roaming User Profiles with diskless systems involves configuring relevant policies and using Folder Redirection.

Although unrelated to Roaming User Profiles, the Offline Folders feature affects diskless systems similarly. Disabling this feature avoids the same effects.

On the domain controller, use the Microsoft Management Console with the Group Policy snap-in to configure the domain policies for the following objects.

Configuring roaming user profiles

Configuring Roaming User Profiles for diskless systems enables roaming without having to download potentially large files in the profile.

On the domain controller, use the Microsoft Management Console with the Group Policy snap-in to configure the domain policies for the following objects.

To prevent the accumulation of Roaming User Profiles on a virtual disk:

OBJECT	COMPUTER CONFIGURATION\ADMINISTRATIVE TEMPLATES\SYSTEM\LOGON
Policy	Delete cached copies of roaming profiles.
Setting	Enabled

To exclude directories with potentially large files from download:

OBJECT	USER CONFIGURATION\ADMINISTRATIVE TEMPLATES\SYSTEM\LOGON, LOG OFF
Policy	Exclude directories in roaming profile
Setting	Enabled
Properties	Prevent the following directories from roaming with the profile: Application Data; Desktop; My Documents; Start Menu.

Configure folder redirection with roaming user profiles

Using Folder Redirection with Roaming User Profiles and diskless systems retains the availability of user documents.

On the domain controller, use the Microsoft Management Console with the Group Policy snap-in to configure the domain policies for the objects that follow.

To configure folder redirection:

1. Create a network share (\ServerName\ShareName) to contain the redirected user folders.
2. Give **Full Control** permission to everyone for the network share.
3. Enable Folder Redirection.

OBJECT	CONFIGURATION\ADMINISTRATIVE TEMPLATES\SYSTEM\GROUP POLICY
Policy	Folder Redirection policy processing
Setting	Enabled

Redirect the **Application Data** folder.

OBJECT	USERS CONFIGURATION\WINDOWS SETTINGS\FOLDER REDIRECTION\APPLICATION DATA
Properties	Basic or Advanced. Target folder location: \ServerName\ShareName\%username% \Application Data

Redirect the desktop folder.

OBJECT	USERS CONFIGURATION\WINDOWS SETTINGS\FOLDER REDIRECTION\DESKTOP
Properties	Basic or Advanced. Target folder location: \ServerName\ShareName\%username% \Desktop

Redirect the **My Documents** folder.

OBJECT	USERS CONFIGURATION\WINDOWS SETTINGS\FOLDER REDIRECTION\DESKTOP
Properties	Basic or Advanced. Target folder location: \ServerName\ShareName\%username%\My Documents

Redirect the Start Menu folder.

OBJECT	USERS CONFIGURATION\WINDOWS SETTINGS\FOLDER REDIRECTION\DESKTOP
Properties	Basic or Advanced. Target folder location: \ServerName\ShareName\%username%\Start Menu

Disable offline folders

Disabling Offline Folders avoids the unnecessary caching of files on diskless systems with network shares.

On the domain controller, use the Microsoft Management Console with the Group Policy snap-in to configure the domain policies for the object that follows.

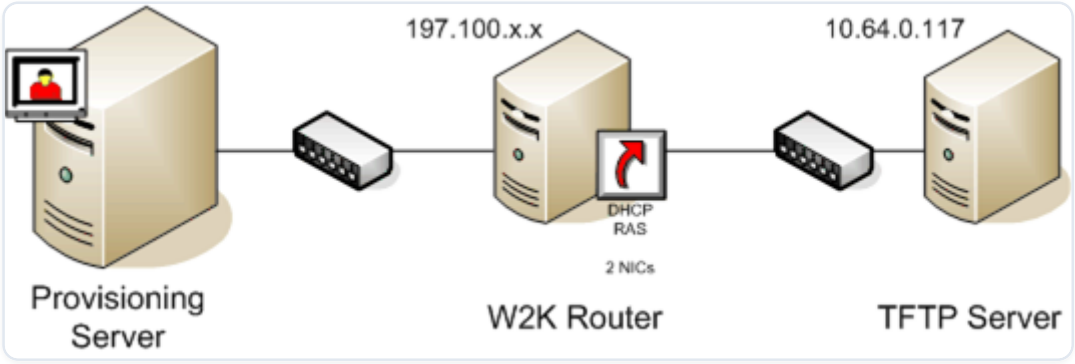
To disable offline folders:

OBJECT	USERS CONFIGURATION\WINDOWS SETTINGS\FOLDER REDIRECTION\DESKTOP
Policy setting	Disable user configuration of Offline Files (Enabled).
Policy setting	Synchronize all Offline Files before logging off (Disabled).
Policy setting	Prevent use of Offline Files folder (Enabled).

Booting through a router

You can boot target devices through a network router. This allows the provisioning server to exist on a different subnet from the target device. Since conditions vary from customer to customer, adjustments are be needed for different network configurations.

The following configuration diagram separates the Provisioning Server from the target device by using a Windows 2000 Server platform acting as a router.



Configuring for DHCP

In this configuration, a DHCP server must be active on the local subnet, `197.100.x.x`, of the target device. In the configuration example above, the DHCP service is running on the same machine acting as a router between the two subnets. It is not mandatory that the DHCP service actually runs on the router itself. This DHCP server provides the IP address and the PXE boot information to the target device.

Configure the DHCP service to provide valid IP addresses to any target device booting on the local subnet, `197.100.x.x`.

To provide the PXE boot information to the target device, configure the following options in your DHCP server:

1. DISABLE Option 60 (Class ID)
2. Enable Option 66 (Boot Server Host Name) – Enter the IP address of the TFTP Server. In this configuration, the value is 10.64.0.10.
3. Enable option 67 (Boot file name) – Enter the name of the boot file. For a standard configuration, the file name is ARDBP32.bin.

Configure Provisioning Services for PXE

Using the console, configure the bootstrap settings to use the **Gateway and Subnet mask** fields. These fields reflect the gateway and subnet to be used by the target device. In this case, they are 197.100.x.x for the gateway, and 255.255.255.0 for the netmask.

Verify the TFTP service is running on the Provisioning Server.

The PXE service on the provisioning server is not necessary since options 66 and 67 in the router's DHCP service provide the same information to the target device. Stop the PXE service on the provisioning server if you have no target devices on the server subnet needing the functionality. The same is true for any DHCP service running on the provisioning server itself.

Running PXE and DHCP on the same computer

If PXE and DHCP are running on the same provisioning server, an option tag must be added to the DHCP configuration. When both are running on the same server, the target devices that the DHCP server is also the PXE boot server. Verify that option tag 60 is added to your DHCP scope. Citrix Provisioning setup automatically adds this tag to your scope as long as the Microsoft DHCP server is installed and configured before installing provisioning. The Configuration Wizard sets-up the Tellurian DHCP Server configuration file if you use the wizard to configure provisioning.

The following is an example Tellurian DHCP Server configuration file which contains the option 60 tag:

```
`max-lease-time 120;
```

```
default-lease-time 120;



option dhcp-class-identifier "PXEClient";



subnet 192.168.4.0 netmask 255.255.255.0 {



option routers 192.168.123.1;



range 192.168.4.100 192.168.4.120;



}`
```

Managing multiple Network Interface Cards (NICs)

Citrix Provisioning can run redundant networks between the servers and the target devices. Redundant networks require both the servers and the target devices be equipped with multiple NICs.

Configure multiple NICs on the target device into a virtual team by using Manufacturer's NIC teaming drivers, or into a failover group using the provisioning NIC failover feature.

NIC Teaming and NIC Failover features provide resilience to NIC failures that occur after the system is up and running. It is only after the OS has loaded that the actual NIC Team or NIC Failover group is established. If NIC failure occurs after being established:

- The NIC Teaming feature allows the system to continue to function because the virtual MAC address is the same as the physical MAC address of the primary boot NIC.
- The NIC Failover feature allows the system to continue to function because it automatically fails over to another NIC that was previously configured for this system.

When using a template with multiple NICs, Citrix Provisioning overwrites the network configuration of the first NIC. All the other NICs' configurations are not changed. For hosts with multiple network resources, the Citrix Virtual Apps and Desktops™ Setup wizard displays available network resources available to the host. It allows you to select the network resource to associate with the first NIC.

Tip:

When a machine powers up, the BIOS goes through the list of available boot devices and the boot order. Boot devices can include multiple PXE-enabled NICs. Citrix Provisioning uses the first NIC in the list as the primary boot NIC, the NIC's MAC address is used as the lookup key for the target device record in the database. If the primary boot NIC is not available at boot time, Citrix Provisioning fails to locate the target device record in the database. Consider that a non-primary NIC only processes the PXE boot phase. A workaround would be to add a separate target device entry for each NIC on each system, and then maintain synchronization for all entries. Citrix does not recommend this process unless the successful startup of a system is considered critical to the continued operation of the system that is already running.

NIC teaming

When configuring NIC teaming, consider the following requirements:

- Citrix Provisioning supports Broadcom, HP branded 'Moon shot' Mellanox NICS and Intel NIC teaming drivers. Broadcom NIC Teaming Drivers v9.52 and 10.24b are not compatible with Citrix Provisioning target device drivers.
- A virtual disk that is built after configuring NIC teaming can run Standard or Private Image Mode.

- Native Windows teaming is not supported on target devices, however, it is supported on Citrix Provisioning servers.
- Teaming of multi-port network interfaces is not supported.
- Multi-NIC is supported for Citrix Virtual Apps™ and Desktops virtual machine desktops. Using the wizard, Citrix Provisioning allows you to select the network to associate with the provisioning NIC (NIC 0). The Delivery Controller provides the list of associated network resources for host connections.
- The target device operating system must be a server-class operating system.
- The new virtual team NIC MAC address has to match the physical NIC that performs the PXE boot.
- NIC teaming software is installed and configured before the target device software.
- Configure NIC teaming and verify that the selected teaming mode is supported by the application and the network topology. It exposes at least one virtual team NIC to the operating system.
- When provisioning machines to an SCVMM server, the setup wizard automatically changes the network configuration of both the first legacy NIC and the second synthetic NIC.
- If changes are required, Citrix Provisioning target device software must be uninstalled before changing the teaming configuration. Reinstall after changes are complete. Changes to teaming configurations on a master target device that has target device software installed results in unpredictable behavior.
- When installing Citrix Provisioning target device software on NT6.x systems within a multi-NIC environment, all available NICs can be used. Therefore bindcfg.exe is no longer required and no longer installed with target device software.

NIC failover

A provisioning target device or server can be configured to support failover between multiple NICs. This feature supports any NIC brand or mixture of brands. Citrix Provisioning supports NIC failover for vDisks in either Standard and Private Image Mode. Consider the following:

- The PXE boot NIC is considered the primary target device MAC address, which is stored in the provisioning database. xxxxx - You define the failover group of NICs when you run the Citrix Provisioning target device installer on the Master Target Device.
- A target device only fails over to NICs that are in the same subnet as the PXE boot NIC.
- Teaming of multi-port network interfaces is not supported with Citrix Provisioning.

- If the physical layer fails, such as when a network cable is disconnected, the target device fails over to the next available NIC. The failover timing is instantaneous.
- The NIC failover feature and Citrix Provisioning high availability feature compliment each other providing network layer failover support. If a failure occurs in the higher network layer, the target device fails over to the next Provisioning Server subject to high availability rules.
- The next available NIC from the failover group is used if the NIC fails and the target device reboots. NICs must be PXE capable and PXE enabled.
- If a virtual NIC (teamed NICs) is inserted into the failover group, the virtual disk becomes limited to Private Image Mode. This functionality is a limitation imposed by NIC teaming drivers.
- By default, Citrix Provisioning automatically switches from legacy Hyper-V NICs to synthetic NICs if both exist in the same subnet. To disable the default behavior (allowing for the use of legacy HyperV NICS even if synthetic NICs exist), edit the target device's registry settings: DisableHyperVLegacyNic"=dword:00000000
- Load balancing is not supported in the NIC failover implementation.

Update NIC drivers

From time to time, upgrade the drivers for your NICs. Follow the guidelines for upgrading NIC drivers.

Upgrade NIC drivers on target devices

To upgrade NIC drivers for target devices:

1. Go to the target device with the original hard drive from which you made the virtual disk image.
2. Set the system BIOS to boot from the hard drive.
3. Reboot the target device directly from the hard drive.
4. Uninstall the target device software from this hard drive.
5. Upgrade NIC driver as directed by the manufacturer's instructions.
6. Reinstall the target device software on the hard drive.
7. Reimage the hard drive to make a new virtual disk image.

> **Note:**

> Do not attempt to upgrade a NIC driver on a virtual disk. Do not attempt to upgrade a NIC driver on a hard disk on which the Provisioning Server is installed. Improperly upgrading a NIC makes the hard drive unable to boot.

Upgrade NIC drivers on a provisioning server

To upgrade NIC drivers on any provisioning server, simply follow the manufacturer instructions for upgrading NIC drivers.

Install the Server component

This installation procedure is for new Citrix Provisioning implementations. For upgrade tasks, see Upgrade. The software can also be installed silently, see Running the configuration wizard silently.

Install any Windows service packs, drivers, and updates before installing the Citrix Provisioning software. From Citrix Provisioning version 2402 LTSR and later CR versions, you can install Citrix Provisioning servers on the system running Windows Server Core. However, currently, you cannot create target VMs on a Citrix Virtual Apps and Desktops™-hosted hypervisor using HDD BDM boot and you cannot do a BDM update using the Citrix Provisioning Console.

> **Note:**
>
> When installing Citrix Provisioning™ software on a server that has previous versions of .NET installed, Citrix recommends rebooting if prompted to do so during the .NET installation.

1. Click the appropriate platform-specific install option. The **Citrix Provisioning Welcome** window appears.
2. Click **Next**. The **Product License Agreement** appears.
3. Scroll to the end to accept the terms in the license agreement, then click **Next** to continue. The **Customer Information** dialog appears.
4. Optionally, type or select your user name and organization name in the appropriate text boxes, then click **Next**. The **Destination Folder** dialog appears.
5. Click **Change**. Enter the folder name or navigate to the appropriate folder where the software is installed. Or, click **Next** to install Citrix Provisioning to the default folder. The **Setup Type** dialog appears.
6. Select the appropriate radio button:

- Complete - Installs all components and options on this computer (default).
- Custom - Choose which components to install and where to install those components.

> **Note:**
>
> Installing the network boot services does not activate them. If you are uncertain about the need for any of these services, choose the **Complete** installation option.

7. Click **Next**.
8. If you select **Complete**, the **Ready to Install the Program** dialog appears. If you selected **Custom**, the **Custom Setup** dialog appears. This dialog provides a **Feature Description** text box that provides a description for the selected component in addition to the space required to install that component.
    - Expand each component icon and select how that component is to be installed.
    - After making component selections, click **Next**. The **Ready to Install the Program** dialog appears. Or, click **Cancel** to close the wizard without making system modifications.
9. On the **Ready to Install the Program** dialog, click **Install** to continue with the installation process. The installation takes several minutes.
10. The *Installation Wizard Completed* message displays in the dialog when the components and options are successfully installed. **Note:** The Installation Wizard can be rerun to install more components later, or rerun on a different computer to install select components on a separate computer.
11. Click **Finish** to exit the Installation Wizard. The **Citrix Provisioning Configuration Wizard** automatically opens.

> **Tip:**
>
> Although Citrix Provisioning does not require a server restart after installing the software, in some instances, a Microsoft message appears to request a restart. When this message appears, configure the farm using the Configuration Wizard, before restarting the server. If this message appears and the server is not restarted, the removeable drive does not appear.

Adding more Citrix Provisioning servers

To add more Citrix Provisioning servers, install the software on each server that is a member of the farm. Run the Installation Wizard, then the Configuration Wizard on each server.

> **Tip:**
>
> The maximum length for the server name is 15 characters. Do not enter the FQDN for the server name.
>
> When the Configuration Wizard prompts for the site to add the server to, choose an existing site or create a site.

After adding servers to the site, start the Citrix Provisioning console and connect to the farm. Verify that all sites and servers display appropriately in the Console window.

Running the configuration wizard silently

Silent product software installs

You can silently install target devices, Citrix Provisioning™ servers, and consoles to a default installation directory using the following command:

```
<Installer Name>.exe /s /v"/qn"
```

To set a different destination, use the `INSTALLDIR` option:

```
<Installer Name>.exe /s /v"/qn INSTALLDIR=D:\Destination"
```

> **Note:**
>
> After performing a silent install of a Citrix Provisioning client, subsequent upgrades using the Upgrade Wizard fail because the client fails to reboot.

Workflow for running the configuration wizard silently

The basic steps involved in the silent configuration of servers in the farm are:

- Create a `ConfigWizard.ans` file from a configured provisioning server in the farm, or create the file manually. To create the file manually, see Create the ConfigWizard.ans file manually.
- Copy the `ConfigWizard.ans` file onto the other servers in the farm, and modify the IP address in the `ConfigWizard.ans` file to match each server in the farm.
- Run `ConfigWizard.exe` with the `/a` parameter on each server.

Enhanced security for Configuration Wizard answer file

The configuration wizard answer files have sensitive fields such as passwords to database and domain accounts. Starting with Citrix Provisioning version 2303, these passwords are protected with enhanced security. Therefore, when you create a new answer file using the Configuration Wizard, provide a passphrase to encrypt passwords. You must use the same passphrase when you use the answer file. You can also continue using your answer files created by the Configuration Wizard prior to Citrix Provisioning version 2303.

Create the `ConfigWizard.ans` file using the Configuration wizard

1. Run ConfigWizard.exe with the `/s` and `/p` parameter on a configured server. Use:
   - `/P` to be prompted for a passphrase
   - `/P:phrase` to provide the passphrase on the command line
2. On the Farm Configuration page, choose **Join existing farm**.
3. On the **Citrix Cloud™** page, select to **Join Citrix Cloud** or **Do not join Citrix Cloud**.
4. Continue selecting configuration settings on the remaining wizard pages, and then select **Finish**.
5. Copy the resulting `ConfigWizard.ans` file from the Citrix Provisioning application data directory in `\\ProgramData\\Citrix\\Provisioning Services`.

Copy and modify the ConfigWizard.ans file

1. For each server, copy the `ConfigWizard.ans` file to the Citrix Provisioning application data directory.
2. Edit the **StreamNetworkAdapterIP=** value so that it matches the IP of the server being configured. If more than one IP is being used for Citrix Provisioning on the server, add a comma between each IP address.

Run the ConfigWizard.exe silently

To configure servers:

Run `ConfigWizard.exe` with the `/a /p` parameter on each server. The parameter `/p` ensures enhanced encryption with a passphrase. The passphrase must be the same that you provided while creating the answer file. For example, use:

- `/P` to be prompted for a passphrase
- `/P:phrase` to provide the passphrase on the command line

> **Note:**
>
> If you use an answer file created with Citrix Provisioning version 2212 or earlier, you can omit `/P`.

> If you join your farm to Citrix Cloud, then you must supply the Citrix Cloud administrator credentials to the Configuration Wizard when using the `/a` option. These credentials are necessary to register or re-register the Citrix Provisioning servers in the farm with Citrix Cloud. To supply the credentials non-interactively, do the following:

1. Create a secure client for your Citrix Cloud administrator account and download the `secureclient.csv` file to your Citrix Provisioning server.
2. On the Citrix Provisioning server, apply the secure client using the `Set-XdCredentials` PowerShell command, choosing the default profile. For example:

   ```
   Set-XDCredentials -SecureClientFile secureclient.csv -CustomerId
   xxxxxxx -ProfileType CloudApi -StoreAs default
   ```

For instructions to create secure clients, see Get started with Citrix Cloud APIs in the Citrix Developer documentation `<https://developer.cloud.com/citrix-cloud/citrix-cloud-api-overview/docs/get-started-with-citrix-cloud-apis/>`.

For more information on Citrix DaaS Remote PowerShell SDK, see `<https://docs.citrix.com/en-us/citrix-daas/sdk-api.html/>`.

For a list of valid `ConfigWizard` parameters:

1. Run `ConfigWizard.exe` with the `/?` parameter.

2. In the Citrix Provisioning application data directory, open the resulting `ConfigWizard.out` file.
3. Scroll to the bottom of the file to view all valid parameters.

To get a list of commands and their descriptions, use the `/ c` parameter.

Create the ConfigWizard.ans file manually

If you want to create the `ConfigWizard.ans` file from scratch, using a text editor that lets you save as Unicode, create a file named `ConfigWizard.ans`, and save it as Unicode. Enter the parameters shown in the table. Include all of the parameters relevant to your configuration.

SCREEN	UI OPTION	MANUAL PARAMETER
DHCP Services	**The service that runs on this computer: Microsoft DHCP**	IPServiceType=0
	Citrix Provisioning BootP service	IPServiceType=1
	Other BootP or DHCP service	IPServiceType=2
	The service that runs on another computer	Not included
PXE Services	**Microsoft DHCP on this computer**	PXEServiceType=0
	Citrix Provisioning PXE service on this computer	PXEServiceType=1
	The service that run on another computer	PXEServiceType=0
Farm Configuration	**Farm is already configured**	FarmConfiguration=0
	Create farm	FarmConfiguration=1
	Join existing farm	FarmConfiguration=2

SCREEN	UI OPTION	MANUAL PARAMETER
Database Server	**DatabaseAdminAuthentication**	DatabaseAdminAuthentication=< *ActiveDirectoryIntegrated or SqlPassword* >
	DatabaseAdminUsername	DatabaseAdminUsername=< *SQL login* > (Used only if DatabaseAdminAuthentication is SqlPassword)
	DatabaseAdminPassword	DatabaseAdminPassword=< *password* > (Used only if DatabaseAdminAuthentication is SqlPassword)
Database Server (after **Create Farm** or **Join existing farm**)	**DatabaseAuthentication**	DatabaseAuthentication=< *ActiveDirectoryIntegrated or SqlPassword* >
	DatabaseUsername	DatabaseUsername=< *SQL login* > (Used only if DatabaseAuthentication is SqlPassword)
	DatabasePassword	DatabasePassword=< *password* > (Used only if DatabaseAdminAuthentication is SqlPassword)
	Server name	DatabaseServer=< *dBName* >, < *NonDefaultSQLPort* > (If default port, omit port value)
	Instance name	DatabaseInstance=< *InstanceName* >
	Database name	DatabaseNew=< *DbName* >

SCREEN	UI OPTION	MANUAL PARAMETER
	Enable MultiSubnetFailover for SQL Server Always On	MultiSubnetFailover=`<` *0 or 1* `>`
	Database Mirror Failover Partner Server Name	FailoverDatabaseServer=`<` *dBName* `>`,`<` NonDefaultSQLPort `>` (If a database mirror failover partner is not used, this value is omitted, or has an empty value)
	Database Mirror Failover Partner Instance Name	FailoverDatabaseInstance=`<` *InstanceName* `>` (If a database mirror failover partner is not used, this value is omitted, or has an empty value)
New Farm (when new farm is created)	**Farm name**	FarmNew=`<` *FarmName* `>`
	Site name	SiteNew=`<` *SiteName* `>`
	Collection name	CollectionNew=`<` *CollectionName* `>`
	Farm Administrator group: PVS server is in Active Directory	ADGroup=`<` *Path to AD group* `>` Ex: `test.local/Users/Domain Users`
	PVS server is in Workgroup	Group=`<` *Path to local group* `>` Ex: PVS-Server-1/Administrators
New Store (when new farm is created)	**Store name**	Store=`<` *StoreName* `>`
	Default path	DefaultPath=`<` *Store path* `>`
Existing Farm (when joining an existing farm)	**Farm name**	FarmExisting=`<` *database name* `>`

SCREEN	UI OPTION	MANUAL PARAMETER
Site (when joining an existing farm)	**Existing site; Site name**	ExistingSite=<*Site name*>
	New site; Site name	Site=<*Site name*>
	Collection name	Collection=<*Collection name*>
Store (when joining an existing farm)	**Existing store; Store name**	ExistingStore=<*Store name*>
	New store; Store name	Store=<*Store name*>
	Default path	DefaultPath=<*Path to store*>
License Server	**License server name**	LicenseServer=<*Citrix License Server's IP, host name, FQDN*>
	License server port	LicenseServerPort=<*LicenseServerPort*> (27000 is default port)
	On-premises (license type)	licenseSKU=0
	Cloud (license type)	licenseSKU=1
	Web services for licensing port	LicenseWebServicesPort=<*LicenseWebServicesPort*> (8083 is default port)
User account	**Network service account**	Network=1
	Specified user account; User name/Domain	<*domain\username*>
	Password	UserName2=<*Password*>
Active Directory Computer Account Password	Days between password updates	PasswordManagementInterval=<*#ofDays*> (Including this parameter enables

SCREEN	UI OPTION	MANUAL PARAMETER
		Automate computer account password updates)
Network Communications	**Streaming network cards**	StreamNetworkAdapterIP=`<` *IPofStreamingNIC1,IPofStreamingNIC2,...* `>` (comma-separated list of IPs)
	Management network card	ManagementNetworkAdapterIP=`<` *IPofManagementNIC* `>` (only one IP)
	Note: Network cards can be both streaming and management.	
	First communications port	IpcPortBase=6890
	Total ports used for server communication	IpcPortCount=20
	Console port	SoapPort=54321
Stream Servers Boot List	**Specify boot servers** (maximum of 4, LS1–LS4)	LS#=<*IP,Default Subnet Mask,Device Gateway,Server Port*>
		For Default Subnet Mask and Device Gateway, use 0.0.0.0 if info is provided by DHCP
		LS1=1.1.1.57,255.255.254.0,10.192.176.1,6910
		LS2=2.2.2.92,0.0.0.0,0.0.0.0,6910
Advanced Stream Servers Boot List	**Verbose mode (Display diagnostic information)**	AdvancedVerbose=<*0 or 1*>

SCREEN	UI OPTION	MANUAL PARAMETER
	Interrupt safe mode (Select if target device hangs during boot)	AdvancedInterruptSafeMode =<0 or 1>
	Advanced Memory Support	AdvancedMemorySupport=<*0 or 1*>
	Network recovery method	AdvancedRebootFromHD=<*0 for Restore Network Connection, 1 for Reboot from hard disk*>
	Recovery time in seconds	AdvancedRecoverSeconds=<*time in seconds*>
	Login polling timeout	AdvancedLoginPolling=<*time in milliseconds*>
	Login general timeout	AdvancedLoginGeneral=<*time in milliseconds*>
Soap SSL Configuration	**SSL port**	SSLPort=54323
	SSL certificate	SSLCert=<*token*>
Problem Report Configuration	**My Citrix Username**	CisUserName=<*username*>
	Password	CisPassword=<*password*>

Install the Console component

The Citrix Provisioning™ console can be installed on any machine that can communicate with the Citrix Provisioning database.

The console installation includes the Boot Device Management utility.

> **Note:**

> If you are upgrading from the current product version, the console software is removed when the Citrix Provisioning server software is removed. Upgrading from earlier versions does not remove the console software automatically.

1. Run the appropriate platform-specific install option; PVS_Console.exe or PVS_Console_x64.exe.
2. Click **Next** on the **Welcome screen**. The **Product License Agreement** appears.
3. Accept the terms in the license agreement, then click **Next** to continue. The **Customer Information** dialog appears.
4. Type or select your user name and organization name in the appropriate text boxes.
5. Enable the appropriate application user radio button, then click **Next**. The **Destination Folder** dialog appears.
6. Click **Change**. Enter the folder name or navigate to the folder where the software is installed, or click **Next** to install the console to the default folder. The **Setup Type** dialog appears.
7. Select the appropriate radio button:
   - Complete - Installs all components and options on this computer (default).
   - Custom - Choose which components to install and where to install those components.
8. Click **Next**.
9. If you select **Complete**, the **Ready to Install the Program** dialog appears. If you selected **Custom**, the **Custom Setup** dialog appears. This dialog provides a *Feature Description* text box that provides a description for the selected component in addition to the space required to install that component. Expand each component icon and select how that component is to be installed. After making component selections, click **Next**. The **Ready to Install the Program** dialog appears. Or, click **Cancel** to close the wizard without making system modifications.
10. On the *Ready to Install the Program* dialog, click **Install** to continue with the installation process. The installation takes several minutes.
11. The *Installation Wizard Completed* message displays in the dialog when the components and options are successfully installed.

Note:

> Rerun the Installation Wizard to install more components later, or rerun on a different computer to install selected components on a separate computer.

Preparing a master target device for imaging

A master target device is a device from which a hard disk image is built and stored on a virtual disk. Citrix Provisioning™ then streams the contents of the virtual disk created from the master target device to other target devices.

Important:

- Citrix® recommends that you install all Windows updates before installing a target device.
- Set up the master target device for the desired workload including IPv6 access if that is required.

This article describes the procedure for preparing the master target device's hard disk. See the following articles for information related to this process:

- Using the Image Wizard to Create a New Disk
- Configuring target devices that use vDisks

Preparing the master target device's hard disk

The master target device is typically different from subsequent target devices because it initially contains a hard disk that is imaged to the virtual disk. If necessary, after imaging, the hard disk can be removed from the master target device.

To support a single virtual disk shared by multiple target devices, those devices must have certain similarities to ensure that the operating system has all required drivers. The three key components that must be consistent are the:

- Motherboard
- Network card, which must support PXE
- Video card

Tip:

> Some platforms, physical or virtual, require a consistent hardware configuration for boot media. For example, if target devices use BDM, the master target matches the BDM configuration because end target devices use that configuration when booting.

> However, the Citrix Provisioning Common Image Utility allows a single virtual disk to simultaneously support different motherboards, network cards, video cards, and other hardware devices.

If target devices share a virtual disk, the master target device serves as a template for all subsequent diskless target devices as they are added to the network. It is crucial to prepare the hard disk of the master target device correctly and to install all software on it in the correct order.

> **Note:**

> Use the following instructions after installing and configuring Citrix Provisioning and creating target devices.

> Software must be installed on the master target device in the following order:

1. Windows operating system
2. Device drivers
3. Service packs updates
4. Target device software

Applications can be installed before or after the target device software is installed. If target devices are members of a domain, and shares a virtual disk, more configuration steps must be completed.

> **Important:**

> Dual boot virtual disk images are not supported.

Configuring a master target device's UEFI

Use the following steps to configure the target device system’s UEFI and the UEFI extension, provided by the network adapter, to boot from the network. Different systems have different UEFI

setup interfaces. If necessary, consult the documentation that came with your system for further information on configuring these options.

1. If the target device UEFI has not yet been configured, reboot the target device and enter the system's UEFI setup. To get to UEFI setup, press the F1, F2, F10 or the **Delete** key during the boot process. The key varies by manufacturer.
2. Set the network adapter to **On** with PXE.

   > **Note:**
   >
   > Depending on the system vendor, this setting appears differently.

3. Configure the target device to boot from LAN or Network first.
4. Save the changes, then exit the UEFI setup program.
5. Boot the target device from its hard drive over the network to attach the virtual disk to the target device.

Installing the master target device software

> **Note:**
>
> Before installing the software on a master target device, clear any UEFI-based-virus protection features. To include antivirus software on the virtual disk image, be sure to turn the antivirus software back on before running the Imaging Wizard.

> Install and configure the OEM NIC teaming software before installing target device software.

On the provisioned target device, start the Windows Device Install service before installing Citrix Provisioning.

Citrix Provisioning target device software components comprise:

- **Citrix Provisioning Virtual Disk**: the virtual media used to store the disk components of the operating system and applications.
- **Citrix Provisioning Network Stack:** a proprietary filter driver that is loaded over the NIC driver, allowing communication between the target devices and the Provisioning Server.

- **Citrix Provisioning SCSI Miniport Virtual Adapter**: the driver that allows the virtual disk to be mounted to the operating system on the target device.
- **Citrix Provisioning Imaging Wizard**: used to create the virtual disk file and image the Master Target Device.
- **Virtual Disk Status Tray Utility**: used to provide general virtual disk status and statistical information. This utility includes a help system.
- **Target Device Optimizer Utility**: used to change target device setting to improve performance.

Citrix Provisioning target device software is available for 32-bit and 64-bit Windows operating systems.

> **Note:**
>
> When installing Citrix Provisioning target device software on NT6.x systems within a multi-NIC environment, all available NICs can be used. Therefore bindcfg.exe is no longer required and no longer installed with target device software.

Installing Citrix Provisioning target device software on a Windows device

1. Boot the master target device from the local hard disk.
2. Verify that all applications on the device are closed.
3. Double-click on the appropriate installer. The product installation window appears.
4. On the **Welcome** dialog that displays, click **Next**, scroll down to the end, then accept the terms of the license agreement.
5. Click **Next** to continue. The **Customer Information** dialog appears.
6. Type your user name and organization name in the appropriate text boxes.
7. Select the appropriate install user option. The selected option depends on whether this application is shared by users on this computer, or whether only the user associated with this computer accesses it.
8. Click **Next**. The **Destination Folder** dialog appears.
9. Click **Next** to install the target device to the default folder, `C:\Program Files\Citrix\Citrix Provisioning`. Optionally, click **Change**, enter the folder name or navigate to the appropriate folder, and then click **Next**, then click **Install**. The installation status information displays in the dialog.

> **Note:**
>
> The installation process takes several minutes. While the installation process is running, you can click **Cancel** to cancel the installation and roll-back any system modifications. Close any Windows Logo messages that appear.

10. The *Installation Wizard Completed* message displays in the dialog when the components and options have successfully been installed. Close the **Wizard** window. If .NET 4.5 or newer is installed and Windows Automount is enabled, the Imaging Wizard starts automatically by default. For details, see Using the Image Wizard to Create a New Disk.

    > **Note:**
    >
    > If a Windows reboot request message displays before the imaging process completes, ignore the request until imaging completes successfully.

11. Reboot the device after successfully installing product software and building the virtual disk image.

Using the Imaging Wizard to create a virtual disk

Use the Imaging Wizard to automatically create the base virtual disk image from a master target device.

Prerequisites

Windows NT 6.x:

The Citrix Provisioning™ Imaging Wizard provides a block-based cloning solution along with the Volume Shadow Copy Service (VSS).

- Each local disk partition is cloned separately to the virtual disk. If there is a separate System Reserved partition on the local disk, it must be included as a source partition.
- Each destination partition must be equal to or larger than the source partition, regardless of the amount of available free space in the source partition. Consider:

- If a larger destination partition is needed, after imaging completes, use Windows disk management "Extend Volume…"
- If a smaller destination partition is needed, before imaging, the source partition can be resized using Windows disk management "Shrink Volume…"

> **Tip:**
>
> If a Windows reboot request message displays before the imaging process completes, ignore the request until imaging completes successfully.

Imaging Wizard limitations

The Citrix Provisioning Imaging Wizard has the following limitations:

- Choose a different name for the target device. This name is different from the host name representing the master VM you are running.
- If the master VM is a domain member, manually create a computer account for it before rebooting the master VM from the generated vDisk.
- Remember to change the cache type of the generated vDisk from **Private** to **Production** before using it to stream target devices.

Imaging

The Imaging Wizard prompts for farm connection information. It includes information necessary to set the appropriate credentials/Active Directory and licensing information. This information is applied to the virtual disk.

1. From the master target device's **Windows Start** menu, select **Citrix>Citrix Provisioning > Imaging Wizard**. The Wizard's **Welcome** page appears.
2. Click **Next**. The **Connect to Farm** page appears.
3. Enter the hostname of a Citrix Provisioning server within the farm. Include the port used to make that connection. If you want to use a numeric IP address, then you must configure the DNS reverse lookup zones to translate the IP address to a hostname.
4. Use the **Windows credentials** (default), or enter different credentials, then click **Next**. If using Active Directory, enter the appropriate password information.
5. On the **Microsoft Volume Licensing** page, select the volume license option to use for target devices. Or, alternately select **None** if volume licensing is not being used.

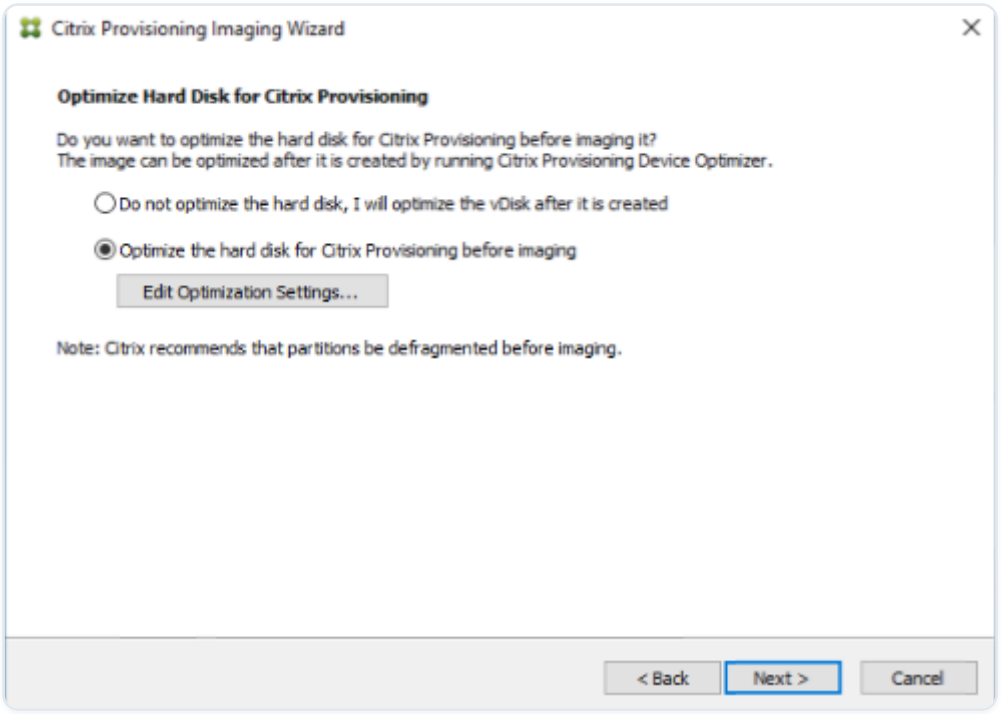
6. Select to create a virtual disk (default), or use an existing virtual disk by entering that virtual disk's name, then click **Next**.
7. If the **Create virtual disk** option was selected, the **New vDisk** dialog displays:
    a. Enter a name for the virtual disk.
    b. Select the **Store** where this virtual disk resides.
    c. Select the **vDisk format** from the appropriate menus. If the VHDX format is **Dynamic**, from the **VHDX block size** menu, select the block size as either **2 MB** or **16 MB**.
    d. Click **Next**, then define volume sizes on the **Configure Image Volumes** page.
8. Click **Next**. The **Add Target Device** page appears.
9. Select the target device name. Include the MAC address associated with one of the NICs. This MAC address that selected when the target device software was installed on the master target device. Also include the collection to add this device to. Click **Next**. If the target device is already a member of the farm, the **Existing Target Devices** page appears.
10. Click **Next**. A **Summary of Farm Changes** appears.
11. Optionally (unless the virtual disk is used to boot the VMs) select to optimize the virtual disk for use with Citrix Provisioning.
12. Verify all changes, then click **Finish**. A confirmation message displays.
13. Click **Yes** on the confirmation message to start the imaging process.

Optimize the hard disk

You can optimize the hard disk before imaging. This process reduces I/O instances to improve write cache functionality.

To access optimization options using the Citrix Provisioning Imaging Wizard:

1. Click the master target device's **Windows Start menu**.
2. Select **Citrix > Citrix Provisioning Device Optimizer**.
3. In the **Optimize Hard Disk for Citrix Provisioning** screen, select **Optimize the hard disk for Citrix Provisioning before imaging**.
4. Click **Edit Optimization Settngs** to access more configuration options.


Citrix Provisioning Imaging Wizard
Optimize Hard Disk for Citrix Provisioning
Do you want to optimize the hard disk for Citrix Provisioning before imaging it?
The image can be optimized after it is created by running Citrix Provisioning Device Optimizer.
Do not optimize the hard disk, I will optimize the vDisk after it is created
Optimize the hard disk for Citrix Provisioning before imaging
Edit Optimization Settings...
Note: Citrix recommends that partitions be defragmented before imaging.
< Back
Next >
Cancel

Upgrade

Citrix Provisioning supports upgrading to the latest product version from versions starting with 7.15.

You can upgrade from any Citrix Provisioning™ version to any latest version. However, upgrade 1912 LTSR CU5 to 1912 LTSR CU6 before upgrading to any later version.

Before upgrading a Citrix Provisioning farm:

- Select a maintenance window that has the least amount of traffic
- Back up the Citrix Provisioning database
- Back up all virtual disks

> **Tip:**
>
> Mirror if you are in a high-availability scenario; for more information, see Database mirroring. No special action is required during the upgrade once the mirroring is set up.

> When upgrading Citrix Provisioning, consider the following:

- Upgrade to the latest licensing server. Note the following when upgrading the license server:
  - License servers are backward compatible and provide the latest security fixes.
  - If necessary, upgrade individual licenses. New features require that the Citrix license has a minimum subscription advantage (SA) date. Validate that your license files have the required license types. See Required license types. You might need to return and reallocate your licenses to have the expected licenses available to support all functions.
- Back up the Citrix Provisioning database. While Citrix always tests to ensure a successful database upgrade, unforeseen circumstances might arise. Citrix strongly recommends backing up the database before upgrading.
- Back up the Citrix Provisioning virtual disk. Citrix recommends backing up the virtual disk before upgrading. This process is only necessary if you plan to use reverse imaging with private images.

- When running the installer to update either the server or console components, if an older version of Citrix Provisioning is detected both components are automatically updated.
- Files located in C:\Program Files\Citrix\PowerShell SDK might be missing after upgrading. This issue occurs because the CDF version used by Citrix Provisioning does not match the version used by other components associated with Citrix Virtual Apps and Desktops. As a result, newer CDF files have a lower version number than previous ones. This issue does not affect the functionality of importing CPV device collections into CVAD machine catalogs. To resolve this issue:

1. Close Citrix Studio.
2. Mount the new Citrix Virtual Apps and Desktops™ ISO.
3. In the mounted ISO, navigate to \x64\DesktopStudio.
4. Right-click PVS PowerShell SDK x64 to expose a contextual menu.
5. Select **Repair**.
6. Run the Repair option. The installation adds the two CDF files as needed.

Upgrade the environment

To upgrade from a previous Citrix Provisioning farm, complete the following procedures:

1. Upgrade consoles. The console is a separate executable that can be installed on upgraded servers (PVS_Console.exe or PVS_Console_64.exe). Citrix recommends upgrading the console, followed by the server software for each provisioning server in the farm. Remote consoles can be upgraded at any time.
2. Upgrade the first provisioning server in the farm, which upgrades the Citrix Provisioning database.
3. Upgrade the remaining provisioning servers within the farm.
4. Upgrade vDisks.

> **Important:**
>
> When upgrading a virtual disk within a Citrix Virtual Apps™ and Desktops deployment, upgrade the master target device software before upgrading the VDA software.

Upgrade utilities

The Upgrade Wizard includes the following utilities:

- The **UpgradeAgent.exe** runs on the target device to upgrade previously installed product software.
- The **UpgradeManager.exe** runs on the provisioning server to control the upgrade process on the target device.

Upgrading at a glance

The information in this section provides step-by-step guidance for upgrading Citrix Provisioning components. For server upgrade information, see the server article. For information about upgrading vDisks, see vDisks.

Upgrade the console and server

Follow these steps to upgrade the console and server:

1. Run the console and server executables to initiate the upgrade process automatically. Citrix recommends that you upgrade the console first, followed by the server.

   > **Tip:**
   >
   > To keep the Citrix Provisioning farm and target devices running during the upgrade process, use the *rolling server upgrade* procedure. This process upgrades one Provisioning Server at a time.

2. The rolling server upgrade performs an upgrade on one server at a time.

   > **Note:**
   >
   > While upgrading the Provisioning Server, it cannot service any target device. Ensure that the remaining servers in the farm support the target devices (clients) during the failover process while the upgrading the server.
   >
   > To perform the *rolling upgrade*, update the first Provisioning Server in the farm:

a. Open the services MSC file (services.msc) and halt the **Citrix PVS Stream Service**. This process causes all provisioning targets connected to this server to fail over to other servers in the farm. Once finished, upgrade the Provisioning Server and console components.

b. Upgrade the Citrix Provisioning database. This process is only done once:

- Use **dbScript.exe** to generate the SQL script. Choose the option to upgrade database and enter the name of the dB. Use that script in SQL Management or SQL command line to upgrade the provisioning database.
- Use the configuration wizard to upgrade the provisioning database; when using this method, consider:
- The Citrix Provisioning Configuration Wizard automatically starts when the **Finish** button is selected after successfully upgrading the Provisioning Server.
- Use the default settings so that the Citrix Provisioning Configuration Wizard uses the previously configured settings. On the Farm Configuration page, select the option **Farm is already configured**. After all configuration information is entered, review the information on the **Finish** page; click **Finish** to begin configuring the provisioning server. At this point, the provisioning database is not configured. A message appears indicating that the database was upgraded. Click **OK** to confirm the message and upgrade the database.
- Verify that Citrix Provisioning processes have started using **services.msc**. Boot a target device to confirm that it can connect to the provisioning server.

Considerations for provisioning database migration using a different SQL server

The Provisioning Console can fail to display the virtual disk attached to a site when migrating a database to a different SQL server. This condition exists when you use the configuration wizard to point to a different SQL server. Despite the console view, the database `dbo.disk` displays the updated virtual disk entries.

To migrate a database:

1. Back up the database.
2. Restore the database on the new SQL server.
3. Run the configuration wizard and retain the default settings on all pages except the database configuration pages.
4. On the **Farm Configuration** page, select **Join existing farm**.

5. On the **Database Server** page, select the new database server and instance names. On the **Farm Configuration** page, the default option is the database imported into the new SQL server.
6. In the configuration wizard, choose the defaults for all other options presented by the wizard.

> **Important:**
>
> During the migration to a different SQL server, do not create a site/store. In the preceding sequence, steps 4 and 5 point to the new SQL server, instance, and database.

Upgrade remaining Provisioning servers

After upgrading the first provisioning server, upgrade the remaining servers in the farm:

1. Open the services MSC file (services.msc) and halt the **Citrix Provisioning Stream Service**. This process causes all provisioning targets connected to this provisioning server to fail over to other provisioning servers in the farm. Once finished, upgrade the provisioning server and console components.

   > **Tip:**
   >
   > Once the server is successfully upgraded, the Citrix Provisioning Configuration Wizard starts automatically after clicking **Finish**. The provisioning database is only updated after upgrading the first provisioning server.

2. Use the default settings. The Citrix Provisioning Configuration Wizard uses the previously configured settings. On the **Farm Configuration** page, make sure that the option **Farm is already configured** is selected. After all configuration information is entered, review the information on the **Finish** page; click **Finish** to being configuring the provisioning server.
3. Repeat these steps to finish upgrading all remaining provisioning servers in the farm.

Rebalance Citrix Provisioning clients

After upgrading and configuring all Citrix Provisioning servers, Citrix recommends that you rebalance all provisioning clients (target devices) within the farm. To rebalance provisioning clients:

1. Start the Citrix Provisioning console and log into the farm.

2. Navigate to the **Servers** tab.
3. Highlight all the provisioning servers that were recently upgraded, right-click to expose a contextual menu.
4. Select **Rebalance clients**.

Upgrade the Citrix Provisioning target device

Citrix Provisioning supports three methods for upgrading target devices:

- In-place upgrade
- Direct VHD\VHDX boot
- Manual upgrade using reverse imaging

Image Portability Service can be used to automate some common Citrix Provisioning operations that cannot be performed while streaming. For more information, see:

- Upgrade PVS: Upgrade PVS takes a VHD(X) from a Citrix Provisioning (PVS) store and upgrades the version of PVS on the image to the version specified in the job request.
- Reverse Imaging: Reverse Imaging takes a VHD(X) from a Citrix Provisioning (PVS) store, and recreates the original platform image. This allows you to perform any upgrade tasks that you must perform with PVS streaming disabled. You can then use the Image Portability Service `Publish` operation to return the image to the PVS environment.

For information on migrating workloads using Image Portability Service, see Migrate workloads between Resource Locations using Image Portability Service.

> **Important:**

> - Citrix strongly recommends backing up the virtual disk if versioning is not used in the upgrade process.

> When using Citrix Provisioning target installers:

- If the system is running, run the new target installer. It must be the same version installed on the target device. This process effectively allows the installer to take care of the upgrade.

In-place upgrades

For in-place upgrades, a maintenance version of the virtual disk is interchangeable with the private image. However, Citrix recommends that you take advantage of Citrix Provisioning versioning to perform an in-place upgrade.

To perform an in-place upgrade:

1. Create a maintenance version of the virtual disk.
2. Using the provisioning console, navigate to the device's properties and set the device type to **Maintenance**.
3. In the **Boot** menu, select **option 1** to boot a client into virtual disk mode using the maintenance version.
4. Log into Windows and run the new target device installer. Install the software and perform a full installation. The target device installer performs the upgrade. Do not run the imaging wizard. Reboot the target device when prompted.
5. Once Windows has loaded, log in to the system and verify that the target device software is the expected version by viewing the status tray. If the status tray is hidden by Windows, locate it by clicking the up arrow on the status tray icon.
6. Shut down the target device.
7. If versioning is invoked, use the provisioning console to promote the maintenance version to test version functionality. Verify the new version and promote it to the production version when it is deemed production quality. Roll this version out to users by rebooting all the target devices using this virtual disk.

Upgrading using VHD\VHDX boot

When using method to upgrade a target device, consider:

- XenServer(formerly Citrix Hypervisor™) only supports .vhd
- Hyper-V 2012 and 2008 R2 only support .vhd
- Hyper-V 2012 R2 and 2016 supports both .vhd and .vhdx

1. Obtain the .vhdx file. Consider:
    - If the virtual disk does not have a version, copy the .vhdx file to the Hyper-V server or import the file to XenServer using **XenCenter® (Files > Import)**.
    - If the virtual disk has a version, perform a base merge and create a .vhdx file in maintenance mode.

2. Perform a direct VHD boot using XenServer®:

   a. Copy the .vhd file to a system running XenCenter and import the file to XenServer using **Files > Import**.

   b. Create a VM using the imported .vhd file. Refer to the *Importing and Exporting VMs* section of the Citrix Virtual Apps and Desktops documentation for more information.

   c. Boot the VM.

   d. Upgrade the target device software. See the information at the beginning of this section for using the Citrix Provisioning target device installers.

3. Perform a direct VHD\VHDX boot using Hyper-V:

   a. Copy the .vhdx file to the Hyper-V server, or

   b. Create a Hyper-V VM using the "Use an existing virtual hard disk" and point to the .vhdx file. For Hyper-V 2012 R2 and 2016, ensure that the generated VM matches those VMs of the virtual disk:

      - Generation 2 = UEFI VMs and systems

      For more information, see Create a virtual machine in Hyper-V.

   c. Boot the VM.

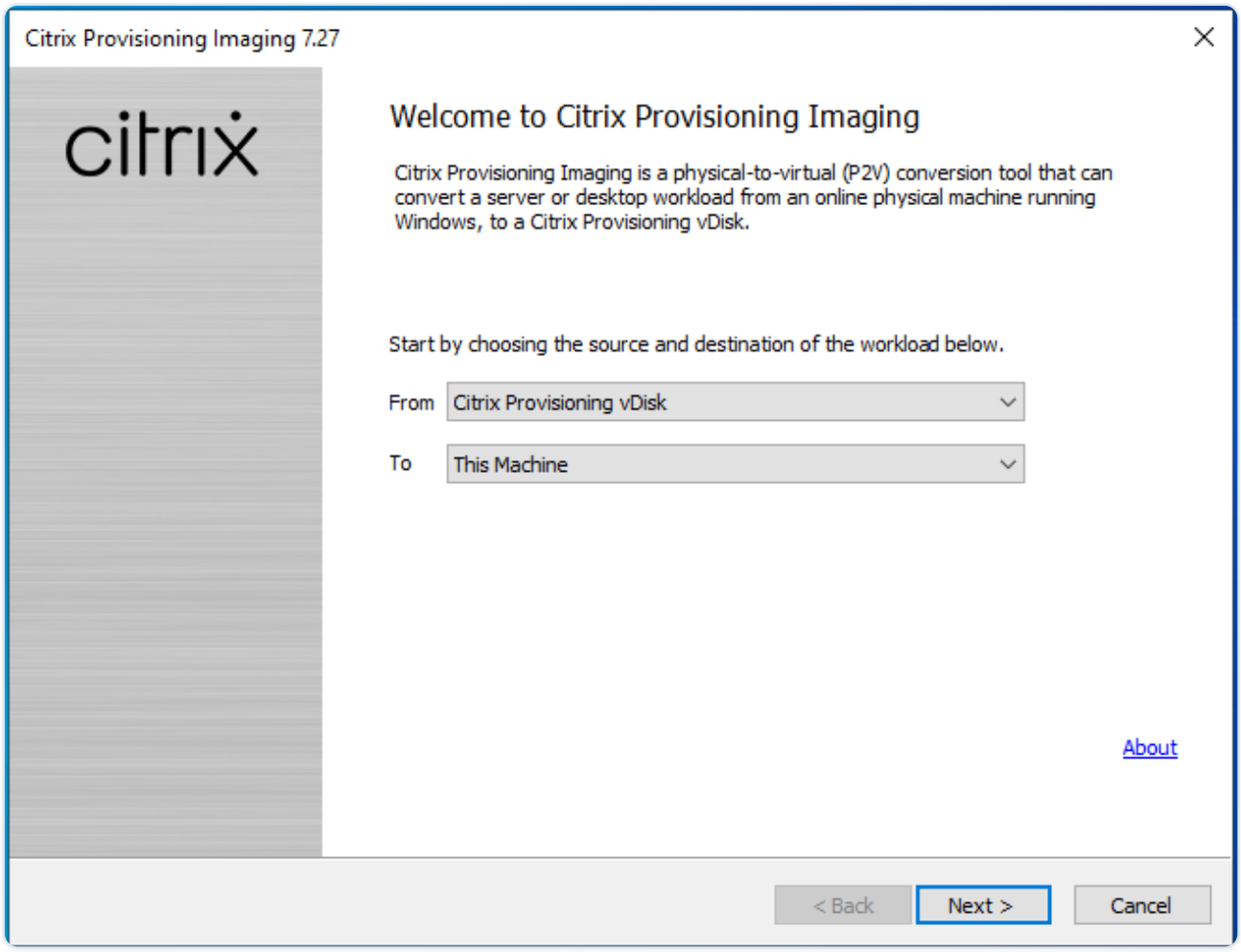
   d. Upgrade the target device software. Upgrade the target device software. See the information at the beginning of this section for using the Citrix Provisioning target device installers.

4. Copy the .vhdx\.vhd file back to the virtual disk store location where it was originally located:

   - If the .vhdx\.vhd file is taken from a based merge version, the file is ready for testing and verification.
   - If the file is copied from the base virtual disk, import the virtual disk into the provisioning database using the **Add or import Existing vDisk** option. Run this option from the virtual disk Pool\Store level in the provisioning console.

Upgrading using manual reverse imaging with P2PVS

Use the information in this section to upgrade Citrix Provisioning using reverse imaging with P2PVS.



The following table illustrates supported upgrade methods:

REVERSE IMAGING METHOD	XEN TOOLS	VM TOOLS	HYPER-V COMPATIBILITY	NIC DRIVER	WINDOWS 10 UPGRADE	ANTIVIRUS UPDATES	FIREWALL/ NETWORK SECURITY SOFTWARE
P2PVS reverse imaging	x	x	x	x	x	x	x
VHD boot from hypervisor	x		x			x	x

REVERSE IMAGING METHOD	XEN TOOLS	VM TOOLS	HYPER-V COMPATIBILITY	NIC DRIVER	WINDOWS 10 UPGRADE	ANTIVIRUS UPDATES	FIREWALL/ NETWORK SECURITY SOFTWARE
Direct VHD boot	x	x	x	x		x	x

1. Boot the Citrix Provisioning target device into the virtual disk using private\maintenance mode.
2. Install **PVS_UpgradeWizard.exe** or **PVS_UpgradeWizard_x64.exe** from the **Upgrade** folder of the ISO image. This folder is located in the latest Citrix Provisioning release area (containing the latest P2PVS.exe file). The upgrade wizard can also be installed through the Citrix Provisioning meta-installer using the **Target Device Installation > Install Upgrade Wizard** option.
3. Run P2PVS.exe from the Citrix Provisioning upgrade wizard directory. By default, this file is located in C:\Program Files\Citrix\Citrix Provisioning Upgrade Wizard.
4. Click the **From** drop-down menu to choose the Citrix Provisioning virtual disk. Click **Next**.
5. In the partition screen, select the partitions undergoing reverse imaging. All system partitions, regardless of whether they have a drive letter or not, are used in reverse imaging. Click **Next**.
6. Click **Convert** on the final page to being reverse imaging.

> **Note:**
>
> When using reverse imaging, consider:
>
> - reverse imaging for UEFI systems is destructive. All partitions on the local hard disk are destroyed and re-created to match those of the virtual disk.

7. Once reverse imaging finishes, reboot the VM from hard disk without network booting.
8. Upgrade the target device. Refer to the information at the beginning of this section for more information.

9. Image the OS to virtual disk again. You can accomplish this imaging by creating a virtual disk or using the existing one.

Using reverse imaging to upgrade Windows 10 machines

To upgrade a Windows 10 image using reverse imaging:

1. Create a target device with a virtual hard disk that is the same size or bigger than the virtual disk.
2. Network boot (PXE/ISO) the VM into the virtual disk using maintenance version or private image mode.
3. Run P2PVS.exe from the Citrix Provisioning target device\ Upgrade Wizard directory. By default, this directory is C:\Program Files\Citrix\Citrix Provisioning, or C:\Program Files\Citrix\Citrix Provisioning Upgrade Wizard, respectively.
4. Click the **From** drop-down menu and choose **Citrix Provisioning vDisk** and click **Next**.
5. In the partition screen, select the partitions for reverse imaging. All system partitions, regardless of whether they have a drive letter or not, are used in reverse imaging. Click **Next**.
6. Click **Convert** on the last page to begin reverse imaging.
7. Once reverse imaging has completed successfully, set the VM to boot from HDD and reboot the VM.
8. Uninstall the Citrix Provisioning target device.
9. Shut down the VM.

> **Note:**
>
> The amount of free space in the c:\ partition. Some used space can be freed up by deleting the **Windows.old** folder in C:\. Refer to the Windows Support page for more information.

10. Judging by the free space on the C:\ partition, increase the size of the VM's hard disk if needed.

> **Note:**

> If this operating system is Windows 10 1607 (code name *Redstone 1* or *Anniversary Update*), Windows 10 update will create another system partition after the C:\\ partition. Currently, it is not possible to increase the size of the C:\\ partition.

11. Boot the VM. Please note the local admin of the VM and remember the local admin password.
12. Run Windows 10 update to upgrade Windows 10.
13. Use local admin credentials to log in since the Windows 10 upgrade process can impact the active directory.
14. Rejoin the VM to the active directory if needed.
15. Install new drivers and more Windows updates if needed.
16. Once updates are done, install Citrix Provisioning target device software.
17. Use the Imaging Wizard or P2PVS to create a virtual disk. The old virtual disk can be used if the size of the VM's virtual hard disk has not been increased in step 11.

Servers

In a Citrix Provisioning™ farm, the database is upgraded at the same time that the first provisioning server is upgraded. After upgrading the database and the first server in the farm, you can upgrade the remaining servers within it. When configuring servers, consider the following:

- While the first provisioning server is being upgraded, some administrative features are not available.
- Citrix recommends closing all Citrix Provisioning consoles until the upgrade is complete to avoid failed operations.
- Upgrade the Citrix Provisioning console and server on every Citrix Provisioning server. After all servers are upgraded, upgrade the console on any other systems it is installed on. The console is not backward compatible.

Upgrading the first provisioning server

> **Important:**

> Uninstall Citrix Provisioning server version 1808 before installing version 1811.

> To upgrade:

1. To upgrade the server and database, run the new version of the server software on the server, then select the **Automatically close and attempt to restart applications** option. If this option is not selected and a **File in use** screen displays, select the **Do not close applications option.**
2. Install the Citrix Provisioning console component on this server or on a server used to manage the farm. For details on installing the console, see the article Installing Citrix Provisioning server software.
3. In the **Configuration Wizard**, select the option to join a farm that is already configured. Running the wizard starts the services. For details, see the instructions on how to join an existing farm in Configuration Wizard Tasks.

Upgrading the remaining Citrix Provisioning servers in the farm

Once you finish upgrading the first server in the farm, use the same procedure to upgrade the remaining servers.

> **Tip:**
>
> The database upgrade is ignored because it was addressed when the first server was upgraded.

Rolling server upgrade

To keep Citrix Provisioning components running during an upgrade, use the rolling server upgrade process. This process upgrades one provisioning server at a time.

> **Tip:**
>
> When upgrading a provisioning server, it cannot service any target device. Due to this constraint, ensure that the remaining provisioning servers in the environment support client failover from the upgraded server.

> To perform the rolling server upgrade, update the first provisioning server in the farm:

1. Open the Services snap-in, `services.msc`, in the MMC and halt the Citrix Provisioning Stream Service. This process causes all targets connected to this provisioning server to fail

over to other servers in the farm. Once finished, upgrade the provisioning server and console components.

2. Upgrade the Citrix Provisioning database. This process is done one time. There are two ways to upgrade the database, using `dbScript.exe` or using the configuration wizard.

Rolling server upgrade using a script

Use `dbScript.exe` to generate a SQL script. Select the option to upgrade the database and enter the name associated with it. Then use the script in SQL Management or the SQL command line to upgrade the provisioning database.

Rolling server upgrade using the configuration wizard

Use the configuration wizard to upgrade the provisioning database. Consider the following:

- The Citrix Provisioning configuration wizard automatically starts when the **Finish** button is selected once the provisioning server has been successfully upgraded.
- Use the default settings. These settings ensure that the configuration wizard retains the settings from the previous instance. On the **Farm Configuration** page, use the option *Farm is already configured*. After collecting and reviewing all configuration information click **Finish** to begin configuring the provisioning server. If the provisioning database has not been upgraded, a message appears indicating that the database is upgraded. Click **OK**.

> **Tip:**

> Verify that Citrix Provisioning is running using the `services.msc` snap-in and boot a target device to confirm it can connect to the provisioning server.

> After upgrading the first provisioning server in the farm, upgrade all other servers:

1. Open the Services snap-in, `services.msc`, in the MMC and stop the Citrix Provisioning Stream Service. This process causes most, if not all, of the target devices connected to this provisioning server to fail over to the server that has been upgraded. Run the new server and console executables to upgrade the server and console components.
2. The configuration wizard automatically starts after clicking **Finish** once the provisioning server has been successfully upgraded.

> **Note:**

> The first provisioning server updates the provisioning database.

3. Use the default settings. These settings ensure that the configuration wizard retains the settings from the previous instance. On the **Farm Configuration** page, ensure that the option *Farm is already configured* is selected. After all configuration information is collected, review the information on the Finish page and click **Finish** to begin configuring the provisioning server.
4. Repeat steps 1–3 to upgrade all other provisioning servers in the farm after upgrading the first server.

Downgrade

If you upgrade to Citrix Provisioning version 2303 and choose to join your farm to Citrix Cloud™, you can then choose to downgrade to an earlier release. However, you cannot downgrade to an earlier release without reverting to the database in use before upgrading.

> **Important:**
>
> You must back up the database before upgrading to Citrix Provisioning version 2303. This restores the database using the original encryption.
>
> To downgrade to an earlier release:

1. Stop all Citrix Provisioning services on all Citrix Provisioning servers in the farm - SOAP, stream process, and Citrix Provisioning API.

On each Citrix Provisioning server in the farm:

1. Uninstall Citrix Provisioning server and console version 2303.
2. Run PoSH script (Downgrade.ps1) to delete registry values. The script disables the features that are included in Citrix Provisioning version 2303 or later.
3. (Optional) Manually deregister the Citrix Provisioning server from Citrix Cloud.
4. Install Citrix Provisioning server and console to a version that you want to downgrade to.
5. Run the Configuration Wizard on a provisioning server. The wizard behaves as if there are no values in the registry. Select **Join Existing Farm** on the **Farm Configuration** dialog to add this provisioning server to an existing farm. Reconfigure the provisioning server.

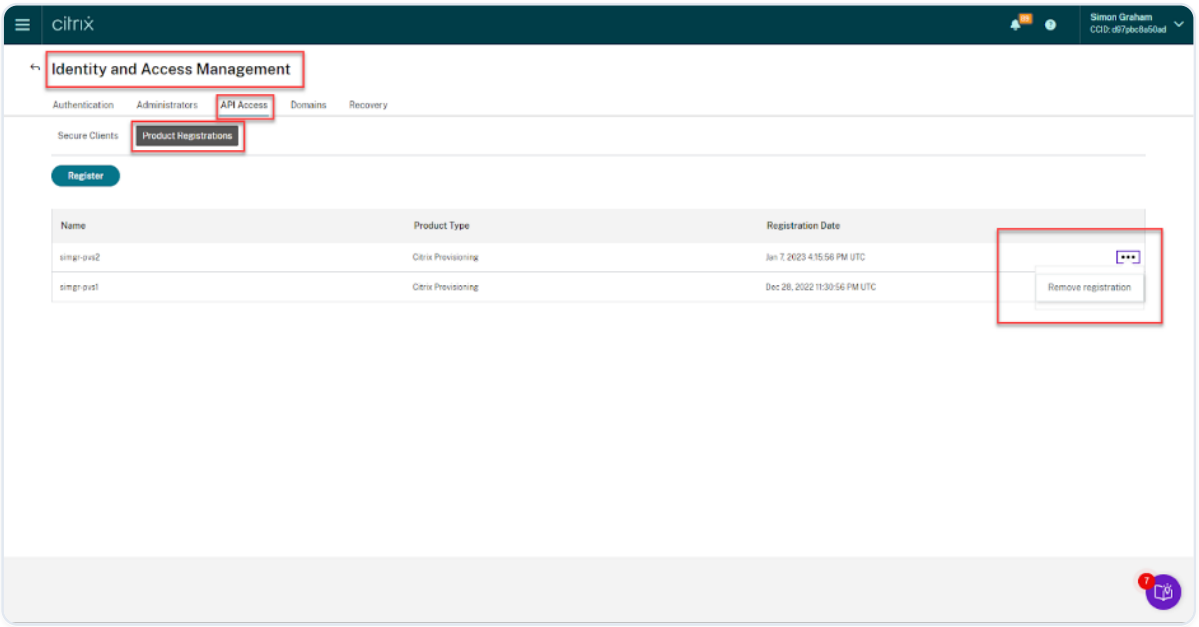
6. Repeat the steps for every Citrix Provisioning server in the farm.

To delete registrations of Citrix Provisioning servers from Citrix Cloud:

1. Stop all Citrix Provisioning services on all Citrix Provisioning servers in the farm - SOAP, stream process, and Citrix Provisioning API.
2. Restore the database from the backup.

On each Citrix Provisioning server in the farm:

1. Run PoSH script (Downgrade.ps1) to delete registry values. The script disables the features that are included in Citrix Provisioning version 2303 or later.
2. (Optional) Manually deregister the Citrix Provisioning server from Citrix Cloud.
   a. Log in to `<customer>.cloud.com` with an administrator account.
   b. Go to **Identity and Access Management > API Access > Product Registrations**.
   c. Use the ••• menu to remove registrations from Citrix Cloud.



3. Run the Configuration Wizard on a provisioning server. The wizard behaves as if there are no values in the registry. Select **Join Existing Farm** on the **Farm Configuration** dialog to add this provisioning server to an existing farm. Reconfigure the provisioning server.
4. Repeat the steps for every Citrix Provisioning server in the farm.

Virtual disks

Upgrading virtual disks involves installing the new version of the Citrix Provisioning™ target device software on the virtual disk image.

> **Important:**
>
> Back up all virtual disks before upgrading to a newer product version.

In-place upgrade

It involves two steps:

1. Start the client in private or maintenance mode.
2. Run the target device installer as described in Preparing a master target device for imaging.

> **Note:**
>
> Upgrading Citrix Provisioning requires local administrator privileges.

Upgrade a virtual disk using reverse imaging

Upgrade by reverse reimaging only if you cannot upgrade using in-place upgrade method.

The reimaging upgrade method that you choose depends on your existing Citrix Provisioning implementation and network requirements.

Versioned virtual disk upgrade

This method reimages to a maintenance version of the virtual disk, allowing production devices to continue running and booting from the production version of the virtual disk. After the upgraded version of the virtual disk is promoted to production, target devices will boot or reboot from the upgraded virtual disk version.

Upgrade prerequisites include:

- Upgrading all Citrix Provisioning servers
- Upgrading Citrix Provisioning consoles

- Creating a backup copy of the virtual disk

To upgrade, complete the following procedure:

1. Boot the Maintenance device from the managed virtual disk while in **Maintenance mode**.
2. From the product installation directory, run `P2PVS.exe` to reverse image using volume-to-volume imaging. Select the virtual disk as the source and the hard disk drive (HDD) as the destination. If your destination partition is on any partition other than partition 1, you must edit the `boot.ini` or `bcedit` partition settings before rebooting from the HDD.
3. Reboot the Maintenance device from the HDD. Do not PXE boot.
4. On the maintenance device, uninstall 6.x target device software, and then install the latest version of the target device software.
5. Run the Citrix Provisioning Imaging Wizard to create a virtual disk image. Create the target device if it does not exist, and assign the virtual disk to the target device.
6. Test streaming the new virtual disk image by booting a maintenance or test device from the upgraded virtual disk.

Manual reverse imaging using P2PVS

When manually performing reverse imaging using P2PVS, consider the following:

- Boot the provisioning target device into the virtual disk using private\\maintenance mode.
- Install `PVS\_UpgradeWizard.exe` or `PVS\_UpgradeWizard\_x64.exe` from the **Upgrade** folder of the ISO image to get the latest `P2PVS.exe`. The upgrade wizard can also be installed with the Citrix Provisioning meta-installer using the Target Device Installation > Install Upgrade Wizard option.
- Run P2PVS.exe from the Citrix Provisioning Upgrade Wizard directory. By default, this directory is C:\\Program Files\\Citrix\\Citrix Provisioning Upgrade Wizard.
- Click the **From** menu and choose **Provisioning Services vDisk** and click **Next**.
- In the partition screen, select the partitions. All system partitions, regardless of whether they have a drive letter or not, are used in reverse imaging. Click **Next**.
- Click **Convert** on the last page to begin reverse imaging.

> **Note:**

> Reverse imaging for UEFI systems is destructive. All partitions on the local hard disk are destroyed and re-created to match the partitions of the virtual disk.

Upgrading vDisks manually

Use the manual upgrade as a universal approach to upgrading vDisks, or if any of the following are true:

- The virtual disk has gone through several modifications in private image mode.
- The original hard drive is no longer available.

The manual upgrade method includes completing the following tasks:

1. Image the virtual disk back to the master target device's hard drive.
2. Install the latest product software on the master target device.
3. Image the target device’s hard drive onto the virtual disk file.
4. Boot from the virtual disk.

Image back to a master target device's hard drive

There are two procedures that allow you to image a virtual disk back to a hard drive. The procedure you select depends on the state of the disk drive you are imaging to. You can image back to the original hard drive from which the virtual disk was created. Returning the image to the original hard drive is the recommended method. Alternatively, you can image back using an unformatted, uninitialized hard disk drive.

Image back to the original hard drive from which the virtual disk was created

1. Boot from the virtual disk in private or shared image Mode.
2. From **Windows Administrative Tools**, select the **Computer Management** menu option. The **Computer Management** window appears.
3. In the tree, under **Storage**, select **Disk Management**.
4. Note the partition letter of the active partition of the original hard disk. If new, format the disk before continuing.
5. Run the **Image Builder** utility on the target device. This utility is at \Program Files\Citrix\Citrix Provisioning\P2PVS.exe.
6. Specify the drive letter of the newly created partition, or the original boot HDD partition, as the **Destination Drive**. The destination drive points to the virtual disk first partition by default.

7. Proceed cloning the hard drive image to the virtual disk destination drive.
8. To connect the virtual disk to the provisioning server, from the console, set the target device to boot from the hard drive, then PXE boot the target device. If this step is not completed properly, the provisioning server is unable to connect with the virtual disk.
9. Uninstall the product software. For details, see the section about removing Citrix Provisioning.

Image back using an unformatted, uninitialized hard disk drive

1. Boot from the virtual disk in **Private Image Mode**.
2. From **Windows Administrative Tools**, select the **Computer Management** menu option. The **Computer Management** window appears.
3. In the tree, under **Storage**, select **Disk Management**.
4. Create a new primary partition, as the first partition, assign a drive letter to it, and then format the partition.
5. Right-click on the newly created partition, then choose **Mark Partition as Active**.
6. Delete the **boot.ini.hdisk** file from the root of the virtual disk.
7. Run the **Image Builder** utility on the target device. This utility is at `\Program Files\Citrix\Citrix Provisioning\P2PVS.exe`.
8. Specify the destination drive letter of the newly created partition, or the original boot HDD partition, as the virtual disk. The virtual disk first points to the destination drive partition by default.
9. Clone the hard drive image to the virtual disk destination drive.
10. To connect the virtual disk to the provisioning server, from the console, set the target device to boot from the hard drive, then PXE boot the target device. If this step is not completed correctly, the provisioning server is unable to connect with the virtual disk.
11. Uninstall the product software. For details, see the section about removing Citrix Provisioning.

Install the master target device software

Complete the following steps to install the latest product software on the master target Device.

1. Run the new Citrix Provisioning Server Target Device installer on the target device.
2. PXE boot the target device.

Image the hard drive

Complete the following steps to image the target device's hard drive onto the virtual disk file:

1. Run the Image Builder utility on the target device. This utility is at \Program Files\Citrix\Citrix Provisioning\P2PVS.exe.
2. Specify the drive letter of the newly created partition, or the original boot HDD partition, as the destination drive. The destination drive points to the virtual disk first partition by default.
3. Clone the hard drive image to the virtual disk destination drive.

Boot from the virtual disk

Using the Citrix Provisioning console, set the target device on the provisioning server to boot from virtual disk, then reboot the target device. The new target device is now running the new virtual disk image.

Upgrade a target virtual disk using in-place upgrade

Use the information contained in this article to upgrade a target device virtual disk using the in-place upgrade method.

> **Important:**
>
> This upgrade procedure can only be used for Citrix Provisioning target devices using version 7.6.1 and newer. For Provisioning Services 7.6.1 and newer, the upgraded target is installed using the *target install method*, and is not upgraded using binary replacement. Citrix recommends that you uninstall if you are using version 7.6.0 or earlier.

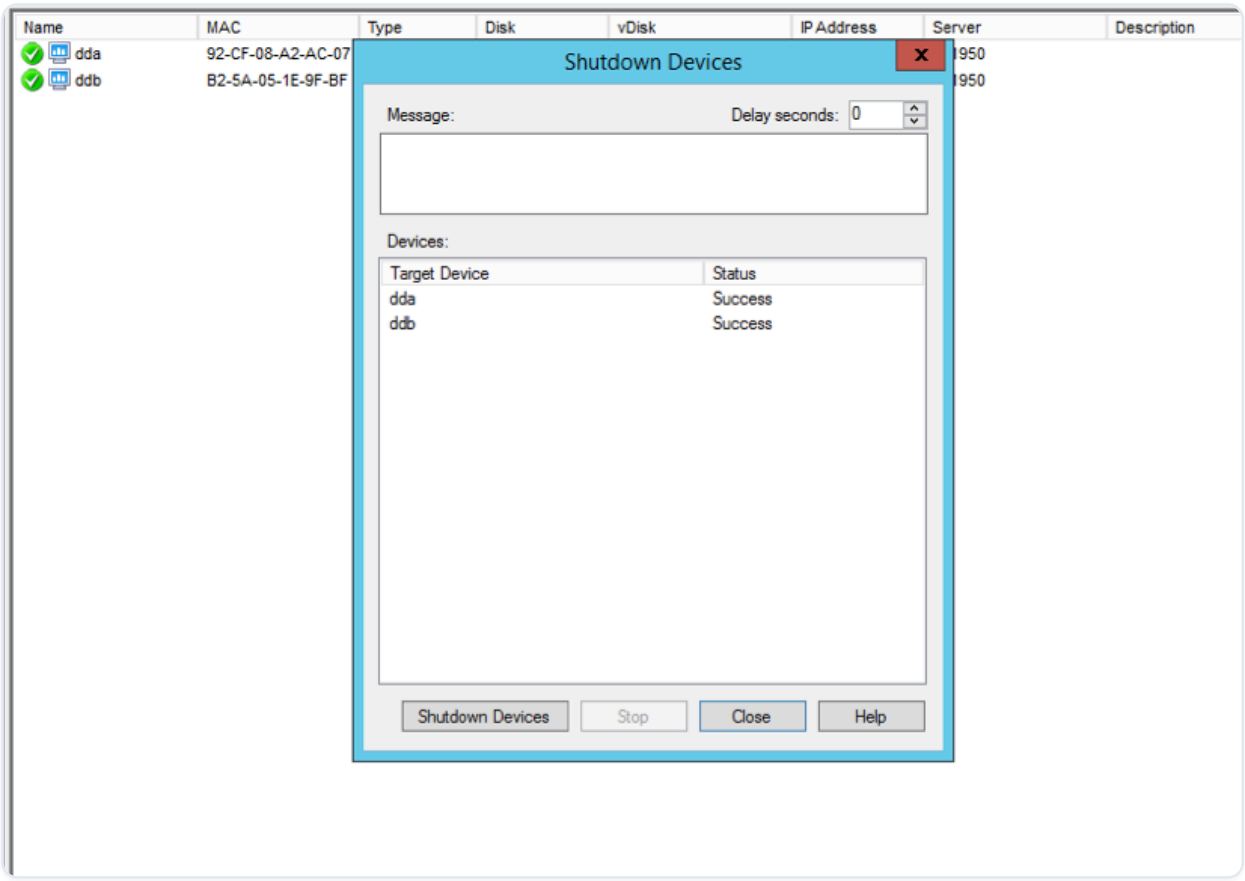
Boot a target device into private image mode or a maintenance version

Use the information in this section to boot a target device in either private image mode, or to boot in maintenance mode.

> **Tip:**
>
> Back up the virtual disk before upgrading before booting from private image mode.

Boot in private image mode

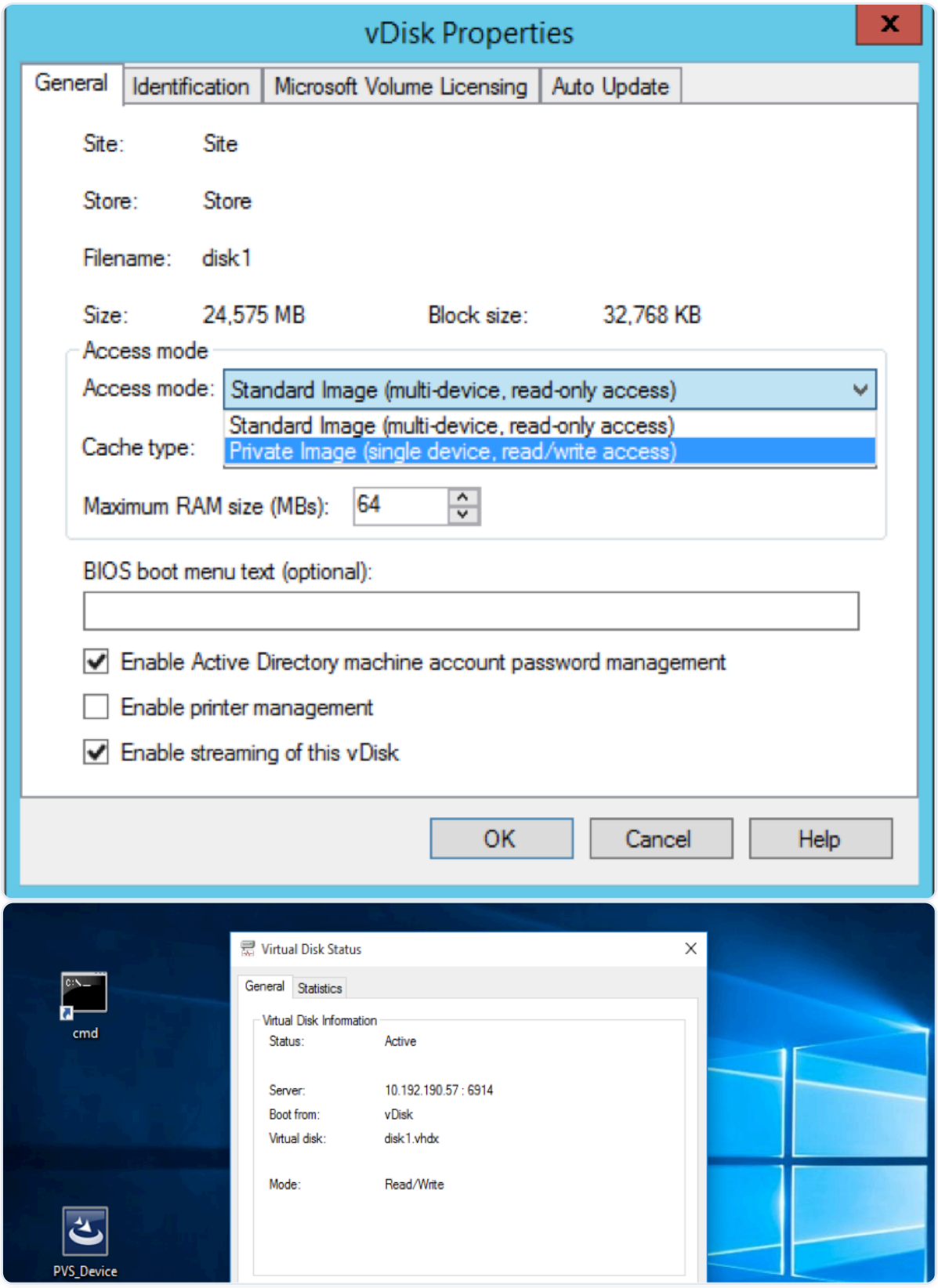
1. Shut down all other devices.



2. Set the virtual disk that you want to upgrade to **private image mode**:

    a. Open the virtual disk's properties dialog by right-clicking the virtual disk, and choose **Properties**.

    b. From the **Access** mode group, select **Private Image** (single device, read/write access):

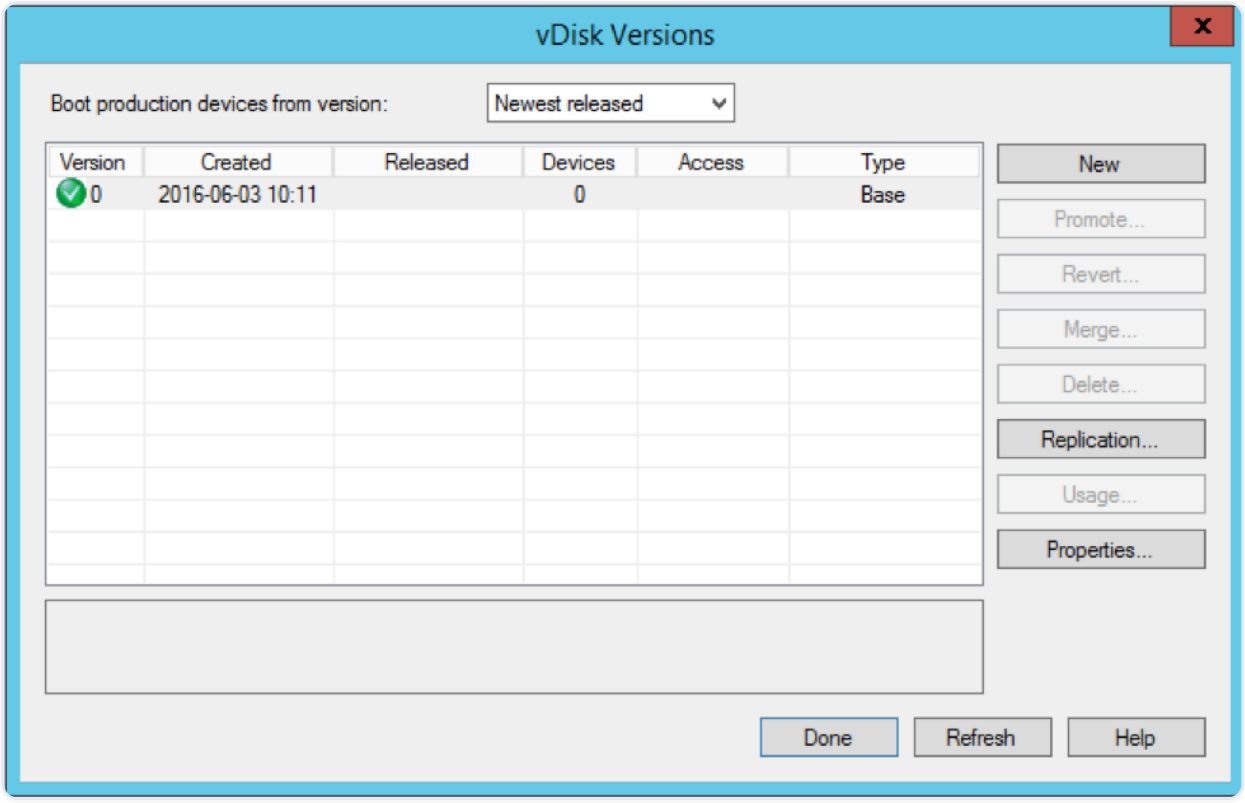


3. Boot a target device using that virtual disk:

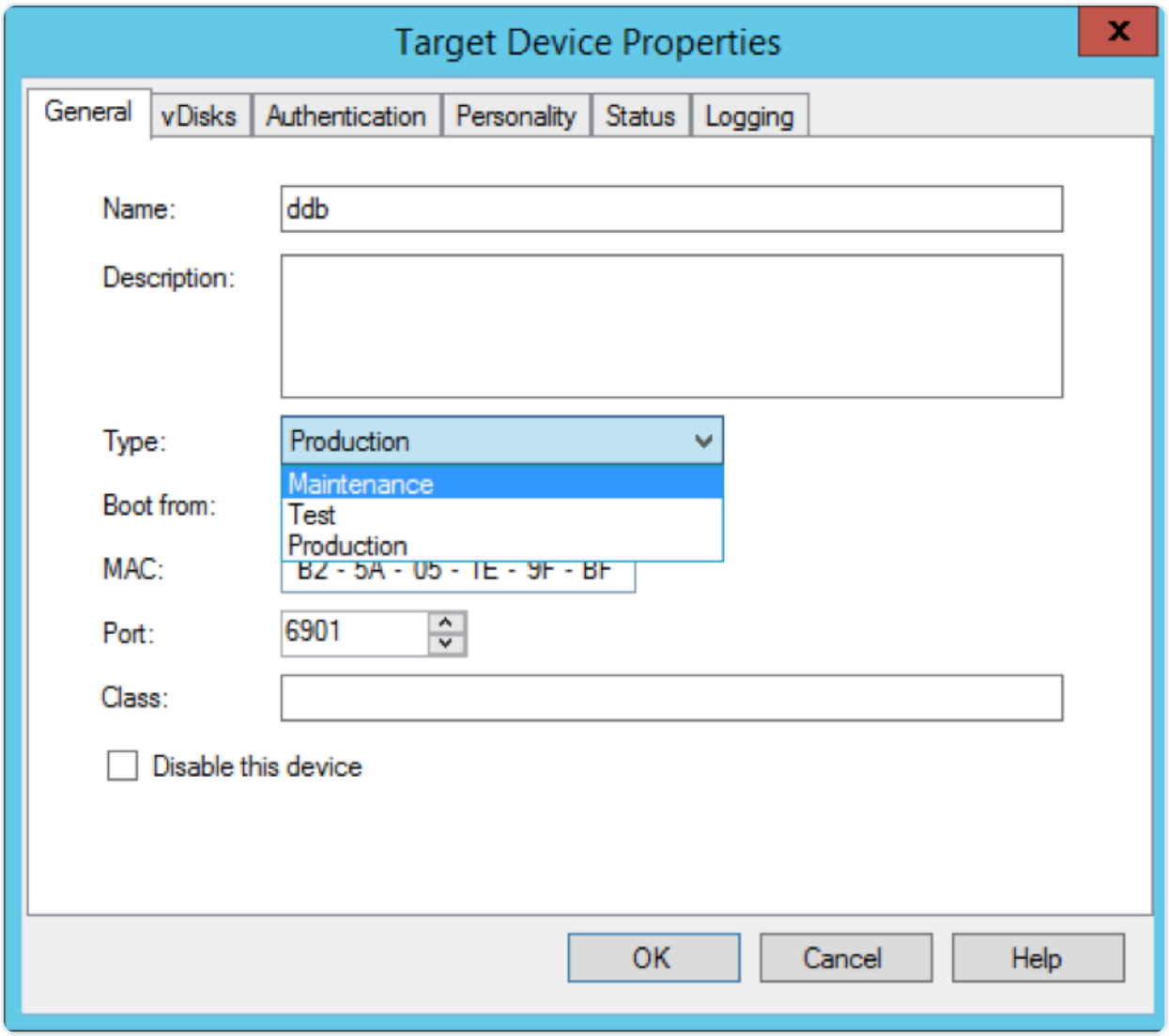
Boot in maintenance mode

1. Right-click the standard mode virtual disk and choose the option **Versions...** to open the virtual disk Versions screen.

2. Click the **New** button (in the upper right portion of the interface) to create a maintenance virtual disk version:



3. Set a target device that is using that virtual disk to maintenance mode by right-clicking on the target, then choose the **Properties** option.
4. Choose **Maintenance** from the menu for the property type:



5. Boot a target device using the specified virtual disk version.
6. Choose **option 1** from the boot menu that appears when booting the target device:

```
Boot device: Network - success.
iPXE (PCI 00:04.0) starting execution...ok
iPXE initialising devices...ok

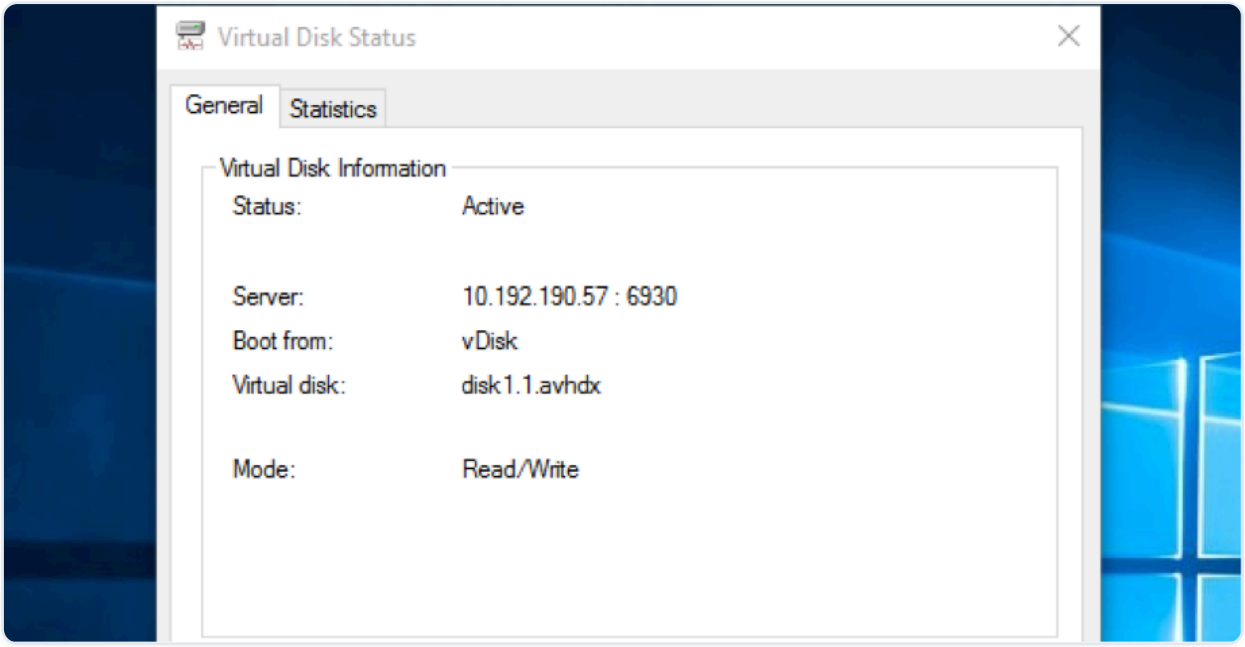


iPXE 1.0.0+ -- Open Source Network Boot Firmware -- http://ipxe.org
Features: HTTP iSCSI DNS TFTP AoE bzImage ELF MBOOT PXE PXEXT Menu

net0: b2:5a:05:1e:9f:bf using rtl8139 on PCI00:04.0 (open)
  [Link:up, TX:0 TXE:0 RX:0 RXE:0]
DHCP (net0 b2:5a:05:1e:9f:bf)... ok
net0: 10.192.190.42/255.255.255.0 gw 10.192.190.1
Next server: 10.192.190.57
Filename: ardbp32.bin
tftp://10.192.190.57/ardbp32.bin... ok


Boot Menu:
----------------------------------------
 1) disk1.1 [maint]
 2) disk1
----------------------------------------
Selection [1-2]:1
```

7. The provisioning status tray of the device resembles:



Tip:

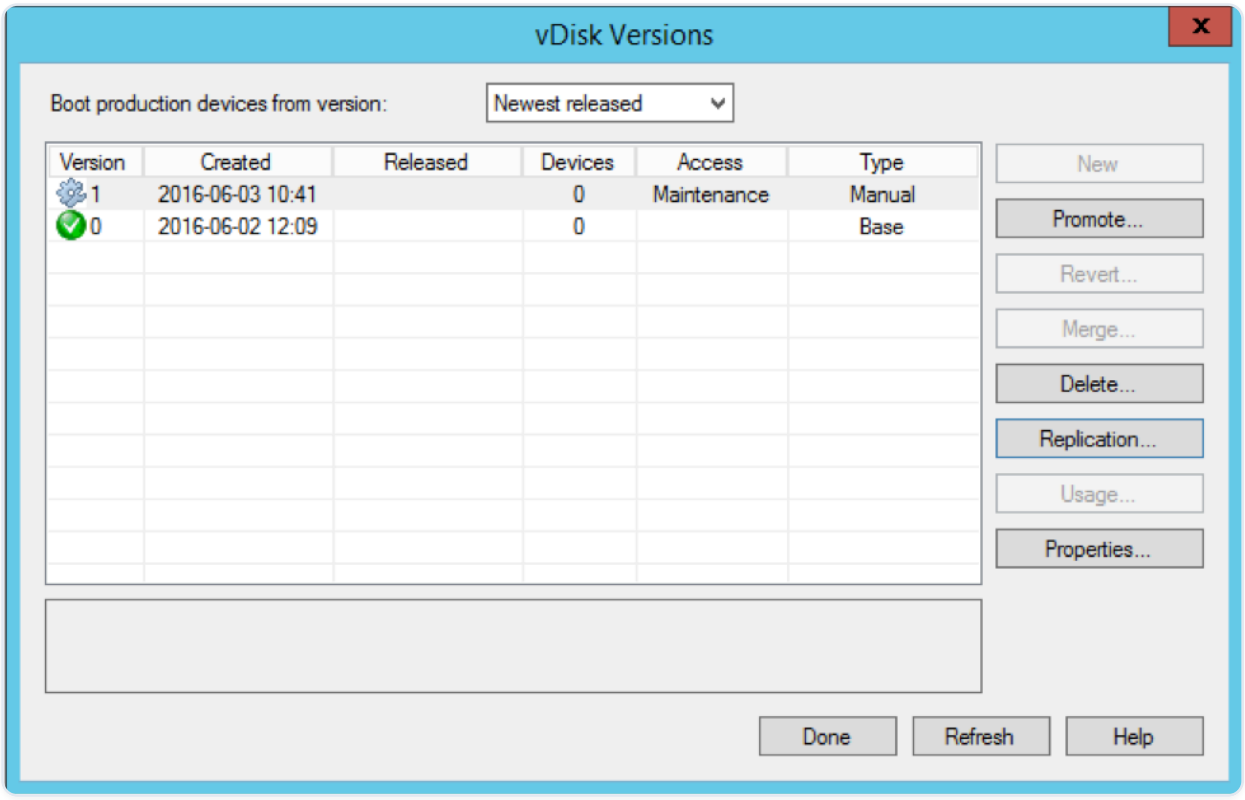
The virtual disk's name is followed by a `.x` where **x** is greater than or equal to 1 and the extension is `.avhdx` or `.avhd`.

Upgrade the Citrix Provisioning target device software

After booting a device into private image mode or a maintenance version, use the information in this section to upgrade the Citrix Provisioning target device software.

To upgrade the Citrix Provisioning target device software:

1. Log into the target device using local administrator login credentials.
2. Copy the PVS_Device.exe or PVS_Device_x64.exe to the target device.
3. Right-click the installer and choose **Run as administrator**.
4. Run the installer and choose all the options as you would install a fresh version.
5. Click **Finish** to begin the upgrade.
6. Shut down the target device.
7. Open the virtual disk version interface.
8. Click **Promote** to promote the virtual disk to either a test or production version:



Tip

The **New** button is grayed out and inaccessible.

a. **Test version** - Use this version to verify the virtual disk is fully operational before promoting it to the production version.

b. **Production version** - Represents the version used by all users in a full roll out of the virtual disk to the production environment.

Configure

Use the information in this section to configure the console, farm, server, device collections, target device, and vDisks. Citrix Provisioning streams a single shared disk image, seen as the virtual disk, in a read-only format to the target device which resides in a collection. These target devices communicate with the Citrix Provisioning server. For more information, see the Citrix Provisioning architecture article.

Console

Use the Citrix Provisioning console to manage components within a provisioning farm. The console can be installed on any machine that can access the farm. For more information, see Using the console.

Starting the Citrix Provisioning™ console

Before starting the console, make sure that the Stream Service is started and running on the Citrix Provisioning server. After the Configuration Wizard runs, the Stream Service starts automatically.

To start the console from the Start menu:

Select **All Programs>Citrix>Provisioning Services > Citrix Provisioning Console**

The console main window appears.

Common console actions

The following menu options are common to most objects in the console:

New Window From Here:

- To open a new console window, right-click on an object in the tree or in the details pane. Select the **New Window from Here** menu option.
- A new console window opens. Minimize the window to view and toggle between one or more windows.

Refresh:

- To refresh information in the console, right-click a folder, icon, or object, then select **Refresh**.

Export List:

1. To export table information from the details pane to a text or comma delimited file, select **Export** from the **Action** menu.
2. Select the location where this file is saved.
3. Type or select the file name in the **File name** textbox.
4. Select the file type from and Save as text boxes.
5. Click **Save** to save the file.

Help: Select an object in the console, then select **Help** from the **Action** menu to display information about that object.

View Options: To customize a console view:

1. Select **View**, then select either **Add/Remove Columns**, or **Customize**.
    - If you selected **Add/Remove Columns**, use the **Add** and **Remove** buttons to select which columns to display.
    - If you selected **Customize** select the check box next to each MMC and snap-in view option that displays in the console window.
2. Click **OK**. The console window refreshes to display the selected options.

Performing tasks in the console

The following menu options are common when performing tasks in the console:

- **Action menu:** Select object-related tasks from the **Action** menu, including boot, restart, send message, view properties, copy, or paste properties.
- **Right-click (context menu):** Right-click a managed object to select object-related tasks. For a complete list of tasks, see that object's management chapter within this guide.
- **Drag and drop:** Using the drag feature, you can quickly perform several common console tasks such as:
    - Move target devices by dragging them from one device collection, and dropping them on another device collection within the same site.
    - Assign a virtual disk to all target devices within a collection by dragging the virtual disk and dropping it on the collection. The virtual disk and the collection must be in the same site.

The new virtual disk assignment replaces any previous virtual disk assignments for that collection.

- Add a target device to a view by dragging the device, then dropping it on the view in console's tree. Drag a provisioning server from one site, then drop it into another site. **Note:** Any virtual disk assignments that were specific to this server and any store information is lost.

- **Copy and paste:** Select an object in the console window, then use the **Copy and Paste** right-click menu options to quickly copy one or more properties of a virtual disk, provisioning server, or target device, to one or more existing vDisks, provisioning servers, or target devices. To copy the properties of a one object type and paste those properties to multiple objects of the same type:

  a. In the tree or details pane, right-click the object which has the properties you want to copy, then select **Copy**. The object-specific **Copy** dialog appears.

  b. Place a check in the check box next to each of the object properties you want to copy, then click **OK**.

  c. In the console tree, expand the directory where the object exists so that those objects display in either the tree or details pane.

  d. Right-click on the object in the tree or details pane that you want to paste properties to, then select **Paste**.

- **Views:** Create views containing target devices to display only those target devices that you are currently interested in viewing or performing tasks on. Adding target devices to a view provides a quick and easy way to perform a task on members of that view, such as: Boot, Restart, Shutdown, Send message.

Views can be created at the site level or at the farm level. To perform a task on members of a view:

1. Right-click on views icon, then select the **Create View** menu option. The **View Properties** dialog appears.
2. Type the name and a description of the new view in the appropriate text boxes, then select the **Members** tab.
3. To add target devices to this view, click the **Add** button. The **Select Target Devices** dialog appears.
4. If you are creating the view at the farm level, select the site where the target devices reside. If you are creating the view at the site level, the site information is already populated.
5. From the menu, select the device collection where you want to add target devices members.

6. Select from the list of target devices that display, then click **OK**.
7. If necessary, continue adding target devices from different device collections within a site.
8. Click **OK** to close the dialog.

For more information on views, see Managing Views.

Configuring the bootstrap from the console

When a Citrix Provisioning server starts a target device, it downloads a boot file using the Citrix Provisioning MBA or PXE-compliant boot ROM. This file must be configured so that it contains the information needed to communicate with the provisioning servers. The **Configure Bootstrap** dialog is used to define the IP addresses for up to four provisioning servers in the boot file.

> **Note:**
>
> For alternative boot methods, see Using the Manage Boot Devices Utility.

> The **Configure Bootstrap** dialog includes the following tabs:

- General
- Target device IP
- Server lookup
- Options

General tab

FIELD	DESCRIPTION
Bootstrap file	The currently selected boot file. If you want to select a different boot file to configure, click the **Add** button or **Read Servers** from the **Database** button.
IP settings	The IP Address, Subnet Mask, Gateway, and Port for up to four provisioning servers, which performs login processing.

FIELD	DESCRIPTION
Add	Click the **Add** button to include a new provisioning server to the file. Specify up to four provisioning servers.
Edit	Highlight an existing provisioning server from the list, then click the **Edit** button to edit this server's IP settings.
Remove	Select an existing provisioning server from the list, then click the **Remove** button to remove this server from the list of available provisioning servers.
Move up and move down	Select an existing provisioning server, and click to move up or down in the list of servers. The order in which the servers appear in the list determines the order in which the servers are accessed if a server fails.
Read servers from database	To populate the boot file with the **Stream Service IP** settings already configured in the database, click the **Read Servers** from **Database** button. This process clears the list then populates the list with the first four servers found in the database.

Target device IP tab

FIELD	DESCRIPTION
Use DHCP to retrieve target device IP	Select this option to retrieve target device IP; default method.
Use static target device IP	Selecting this method requires that you identify a primary and secondary DNS and domain.

Server lookup tab

- **Use DNS:** Select this option to use DNS to find the server. The host name displays in the Host name textbox. If this option is selected along with **Use DHCP to retrieve Device IP option**, configure the DHCP server to provide the DNS server.

  > **Note:**
  >
  > If using high availability, specify up to four provisioning servers for the same Host name on your DNS server.

- **Use static IP:** Use the static IP address of the provisioning server from which to boot from. If you select this option, click **Add** to enter the following server information, then click **OK** to exit the dialog: IP Address, Subnet Mask, Gateway, Port (default is 6910).

  > **Note:**
  >
  > If using high availability (high availability), enter up to four provisioning servers. If you are not using high availability, only enter one. Use the **Move Up** and **Move Down** buttons to sort the servers boot order. The first one listed is the server that the target device attempts to boot from.

Options tab

FIELD	DESCRIPTION
Verbose mode	Select the Verbose Mode option if you want to monitor the boot process on the target device (optional) or view system messages.
Interrupt safe mode	Select **Interrupt Safe Mode** if you are having trouble with your target device failing early in the boot process.
Advanced memory support	This setting enables the bootstrap to support newer Windows OS versions and is enabled by default. Only disable this setting if your target

FIELD	DESCRIPTION
	device is hanging or behaving erratically in early boot phase.
Network recovery method	This field includes: **Restore Network Connections**. Selecting this option results in the target device attempting indefinitely to restore its connection to the provisioning server. **Reboot to Hard Drive**, a hard drive must exist on the target device. Selecting this option instructs the target device to perform a hardware reset to force a reboot after failing to re-establish communications. The user determines the number of seconds to wait before rebooting. Assuming the network connection cannot be established, PXE fails, and the system reboots to the local hard drive. The default number of seconds is 50, to be compatible with high availability configurations.
Logging polling timeout	Enter the time, in milliseconds, between retries when polling for provisioning servers. Each server is sent a login request packet in sequence. The first responding server is used. In systems that are not highly available, this time-out simply defines how often to retry the single available provisioning server with the initial login request. This time-out defines how quickly the round-robin routine switches from one server to the next in trying to find an active one. The valid range is from 1,000 milliseconds to 60,000 milliseconds.
Login general timeout	Enter the time-out, in milliseconds, for all login associated packets. Do not include the initial login polling time-out. This time-out is longer than the polling time-out. The server needs time to contact all associated servers, some of which are down and requiring retries and time-outs from the server to the other servers. This process determines if they are online or not.

FIELD	DESCRIPTION
	The valid range is from 1,000 milliseconds to 60,000 milliseconds.

Configuring the bootstrap file

1. In the console, select a provisioning server within the **Servers** folder in the tree, then select **Configure bootstrap** from the **Actions** pane or the context menu. The **Configure Bootstrap** dialog appears.

   Select the boot file that was copied to the directory you selected during the Citrix Provisioning server setup. The server returns the list of bootstrap files found under **Citrix Provisioning Program Data**. As a result, the server must be active for the **Configure Bootstrap** menu item to appear.

   Important:

   If a previous version of Citrix Provisioning was installed on this server, you must change the default location from:

   ```
   C:\\Program Files\\Citrix\\Citrix Provisioning
   ```

   to:

   ```
   C:\\Documents and Settings\\All Users\\Application Data\\Citrix\\Citrix Provisioning\\Tftpboot
   ```

   If the default is not changed, the bootstrap file cannot be configured from the console and target devices fail to boot. A ‘Missing TFTP’ error message appears.

   If you installed the console on a separate machine, select the path of the remote provisioning server (which has boot services installed).

2. The Configuration Wizard writes the list of IP addresses to the database for the server. Selecting **Read Servers from the Database** gets the first IP and port for the server and populates it into the list. This step is performed when the list is blank, or to replace the whole list with new values. These values are set in the **Streaming network cards** section of the Configuration Wizard's Network Communications page. Citrix Provisioning uses the first network card selected.

3. Choose from the following options:

    - Optionally select the **Verbose Mode** option if you want to monitor the boot process on the target device. This option enables system messaging on the target device.
    - Select **Interrupt Safe Mode** if the target device hangs early in the boot process.
    - Select the **Advanced Memory Support** option to enable the bootstrap to support newer Windows OS versions. Advanced Memory Support is enabled by default. Only disable this setting if your target device is hanging or behaving erratically in early boot phase.

4. Select from the following Network Recovery Methods:

    - Restore Network Connections - Selecting this option results in the target device attempting, indefinitely, to restore its connection to the Citrix Provisioning server.
    - Reboot to Hard Drive - Selecting this option instructs the target device to perform a hardware reset. This process forces a reboot after failing to re-establish communications for a defined number of seconds. The user determines the number of seconds to wait before rebooting. Assuming the network connection cannot be established, PXE fails, and the system reboots to the local hard drive. The default number of seconds is 50. Click the **Browse** button to search for and select the folder created in Step 1, or enter a full path or UNC name.

    > **Important:**
    >
    > If the partition containing the vDisks is formatted as a FAT file system, a message displays a warning, resulting in suboptimal performance. Citrix® recommends that you use NTFS to format the partition containing the vDisks. Do not change the address in the **Port** field.
    >
    > All boot services (PXE, TFTP) must be on the same NIC (IP). But the Stream Service can be on a different NIC. The Stream Service allows you to bind to multiple IPs (NICs).

5. Configure the following:

    Login Polling Timeout

    Enter the time, in milliseconds, between retries when polling for servers. Each server is sent a login request packet in sequence. The first responding server is used. This time-out simply defines how often to retry the single available server with the initial login request. This time-out

defines how quickly the round-robin routine switches from one server to the next, in trying to find an active server. The valid range is from 1,000 milliseconds to 60,000 milliseconds.

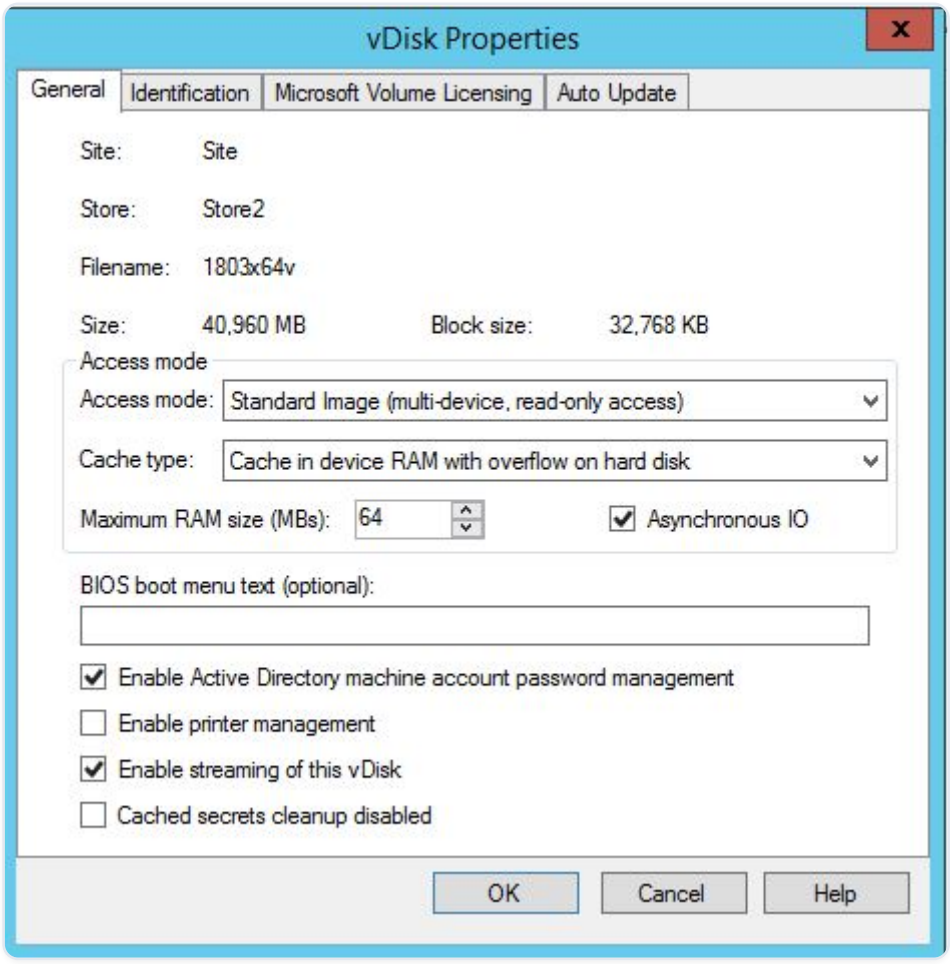
Login General Timeout

Enter the time-out, in milliseconds, for all login associated packets. Do not include the initial login polling time-out. The valid range is from 1,000 milliseconds to 60,000 milliseconds.

6. Click **OK** to save your changes.

Enable asynchronous I/O using the Citrix Provisioning console

Enable Asynchronous I/O streaming functionality for a virtual disk directly from the provisioning console. In the virtual disk properties screen, select **Asynchronous IO**.



Tip:

For more information, see Improving performance with asynchronous I/O streaming.

Farm

Use the information in this section to configure a farm using the Citrix Provisioning™ console. This section includes information about the following elements:

- General tab
- Security tab
- Groups tab
- Licensing tab
- Options tab
- Virtual disk Version tab
- Status tab
- Registration tab
- Encryption tab

The tables that follow identify and describe properties on each tab of the **Farm Properties** dialog.

General tab

FIELD	DESCRIPTION
Name	Enter or edit the name of this farm.
Description	Enter or edit a description for this farm.

Security tab

FIELD	DESCRIPTION
Add	Click **Add** to apply farm administrator privileges to a group. Select each box next to the groups to which you want to apply farm administrator read-only privileges.
Remove	Select the groups that you want to remove from the administrator role. Click **Remove** to remove the selected groups.

Groups tab

FIELD	DESCRIPTION
Add button	Click the **Add** button to open the **Add System Groups** dialog. To display all security groups, leave the text box set to the default `*`. To display groups, type part of the name using wildcards `*`. For example, if you want to see `MY_DOMAIN\Builtin\Users`, type: `User*`, `Users`, or `ser`. However, if you type `MY_DOMAIN\Builtin*`, you get all groups, not just those groups in the MY_DOMAIN\Builtin path. Select the check boxes next to each group included in this farm. **Note:** Filtering on groups was introduced in 5.0 SP2 for efficiency purposes.
Remove button	Click the **Remove** button to remove existing groups from this farm. Highlight the groups to which privileges do not apply.

Licensing tab

FIELD	DESCRIPTION
License server name	Enter the FQDN of the license server, a hostname, or an IP address if that is supported by the license server.
License server port	Enter the port number that the license server uses or accept the default, which is 27000.
Web Services for Licensing Port	Enter the port number that the web services for licensing uses or accept the default, which is 8083.

FIELD	DESCRIPTION
Select Citrix Provisioning license type	Select one of the license types. **Note:** • If you have a DaaS (Citrix Cloud™) license, then select **Citrix Cloud**. • If you have an on-premises Citrix Virtual Apps and Desktops™ license or are operating independently of Citrix Virtual Apps and Desktops, then select **Citrix Virtual Apps and Desktops**.

Options tab

FIELD	DESCRIPTION
Auto add	When using this feature, select the site used by new target devices. If the **No default site** is chosen, the site of that Citrix Provisioning server that logs in the target device is used. Use the **No default site** setting if your farm has site scoped PXE/TFTP servers. **Important:** Enable this feature when adding new target devices. Enabling this feature results in computers being added without the approval of a farm administrator.
Auditing	Enable or disable the auditing feature for this farm.

FIELD	DESCRIPTION
Offline database support	Enable or disable the offline database support option. This option allows servers within this farm to use a snapshot of the database in case the connection is lost.

Note:

The **Send anonymous statistics and usage information** checkbox, which enables the Customer Experience Improvement Program (CEIP), is no longer available.

Virtual disk version tab

FIELD	DESCRIPTION
Alert if number of versions from base image exceeds	Set an alert if the number of versions from the base image is exceeded.
Default access mode for new merge versions	Select the access mode for the virtual disk version after a merge completes. Options include; Maintenance, Test (default), or Production. **Note:** If the access mode is set to **Production** and a test version exists, the state of the resulting auto-merged version is automatically set to *Maintenance* or *Test*. If a Maintenance version exists, an automatic merge is not performed.
Merge after automated virtual disk update, if over alert threshold	Enable automatic merge. Enable the automatic merge feature if the number or virtual disk versions exceeds the alert threshold. Minimum value is 3 and maximum value is 100.

Status tab

FIELD	DESCRIPTION
Status of the farm	Provides database status information, information on group access rights being used, and information on joining status of farm to Citrix Cloud or a Citrix Virtual Apps™ and Desktops site.

Registration tab

FIELD	DESCRIPTION
State	If you are joining your farm to Citrix Cloud, then this field provides information on the joining status of your farm to Citrix Cloud and customer ID and name. If you are joining your farm to a Citrix Virtual Apps and Desktops site, then this field provides information on the joining status of your farm to a Citrix Virtual Apps and Desktops site, and site name.
Unregistered servers	Lists the servers in the farm that are not yet registered to Citrix Cloud or a Citrix Virtual Apps and Desktops site.

Encryption tab

The tab is available only after you choose to join your farm to Citrix Cloud. Using this tab, you can:

- Monitor the status of the database key rotation
- See the list of Citrix Provisioning servers that are waiting on key distribution
- Rotate the encryption key

Key rotation distributes a new database encryption key to all the Citrix Provisioning servers in the farm. After the distribution is complete, the database is re-encrypted with this new key. This process ensures enhanced database security.

FIELD	DESCRIPTION
State	States of the encryption that are Distributing keys, Re-encrypting Database, and Idle.
Offline servers	Lists the servers in the farm that are offline.

The description of the states of the encryption are as follows:

Distributing Keys: This is the first state of key rotation. In this state, the new database encryption key is being synchronized with all the Citrix Provisioning servers. The farm remains in the Distributing Keys state until all the servers have the latest encryption key. To retrieve the new encryption key, a Citrix Provisioning server:

- must be active (that is, must not be offline) till it gets the new encryption key. You can turn off the server once it gets the new encryption key
- can communicate with the Citrix Cloud to get the encryption key

Re-encrypting Database: This is the next state after **Distributing Keys**. In this state, after all the Citrix Provisioning servers in the farm get the new encryption key, the encrypted fields in the database are re-encrypted with this new encryption key.

Idle: This is the next state after re-encrypting the database. This state implies that the key rotation process is complete. The **Rotate Encryption Key** button is enabled when the encryption status is **Idle**. After you click **Rotate Encryption Key**, the state changes to **Distributing Keys**.

Note:

- Each encryption key cycling job takes a minimum of 5 to 10 minutes to move to the next state. However, the process is delayed if there are offline Citrix Provisioning servers.
- You might see a Citrix Provisioning server that initiated the key rotation in the list of servers that are waiting on key distribution even after the server in the farm gets the new encryption key immediately. Wait for approximately 5 minutes for that server to finish its key rotation process, after which it moves out of the list.
- You cannot add new Citrix Provisioning servers in the farm when the state is **Distributing Keys** or **Re-encrypting Database**.

Using PowerShell and MCLI commands to rotate encryption key

You can now use PowerShell and MCLI commands to rotate encryption keys. Before using the commands, make sure that:

- All Citrix Provisioning servers in the farm are registered with the Citrix Cloud
- Encryption status is **Idle**

Using PvsPsSnapIn:

1. Open the **PowerShell** window.
2. Install the PowerShell Snap-In. The path where the `Citrix.PVS.SnapIn.dll` is installed is: `C:\Program Files\Citrix\Provisioning Services Console\Citrix.PVS.SnapIn.dll`
3. Run `Start-PvsRotateEncryptionKeys` to start the key rotation process. After you run the command, the key rotation status changes to **Distributing Keys**.

   > **Note:**
   >
   > If you run the command `Start-PvsRotateEncryptionKeys` when the key rotation status is `Distributing Keys` or `Re-encrypting Database`, you get an error because the key rotation is in process and keys can be rotated only when the key rotation status is **Idle**.

4. Run `Get-PvsKeyRotationPendingServers` command to get the list of servers in the farm that are waiting on key distribution and servers that are offline.

   > **Note:**
   >
   > - When the key rotation status is:
   >   - **Distributing Keys**, you get the list of servers that are waiting on key distribution.
   >   - **Re-encrypting Database** or **Idle**, you get the list of servers that are offline.
   > - You might see a Citrix Provisioning server that initiated the key rotation in the list of servers that are waiting on key distribution even after the server in the farm gets the new encryption key immediately. Wait for approximately 5 minutes for that server to finish its key rotation process, after which it moves out of the list.

5. Turn on the servers that are offline. Ensure that the servers in the farm can communicate with the Citrix Cloud to get the encryption key.
6. After the key rotation process is complete, the status of the key rotation must change to **Idle**. Run the command `Get-PvsFarm` to verify the key rotation status. The values of the property `EncryptionStatus`:
    - 0: Idle state
    - 1: Distributing Keys
    - 2: Re-encrypting Database

> **Note:**
>
> Each encryption key cycling job takes a minimum of 5 to 10 minutes to move to the next status. However, the process is delayed if there are offline Citrix Provisioning servers and servers waiting on key distribution.

Using MCLI.exe:

1. Open the **PowerShell** window.
2. Run `.\MCLI.exe Run CycleEncryptionKeys` to start the key rotation process. After you run the command, the key rotation status changes to `Distributing Keys`.

    > **Note:**
    >
    > If you run the command `.\MCLI.exe Run CycleEncryptionKeys` when the key rotation status is **Distributing Keys** or **Re-encrypting Database**, you get an error because the key rotation is in process and keys can be rotated only when the key rotation status is **Idle**.

3. Run `.\MCLI.exe Get PendingServers` command to get the list of servers in the farm that are waiting on key distribution and servers that are offline.

    > **Note:**

- When the key rotation status is:
  - **Distributing Keys**, you get the list of servers that are waiting on key distribution.
  - **Re-encrypting Database** or **Idle**, you get the list of servers that are offline.
- You might see a Citrix Provisioning server that initiated the key rotation in the list of servers that are waiting on key distribution even after the server in the farm gets the new encryption key immediately. Wait for approximately 5 minutes for that server to finish its key rotation process, after which it moves out of the list.

4. Turn on the servers that are offline. Ensure that the servers in the farm can communicate with the Citrix Cloud to get the encryption key.
5. After the key rotation process is complete, the status of the key rotation must change to **Idle**. Run the command `.\MCLI.exe Get Farm -f` to verify the key rotation status. The values of the property `EncryptionStatus`:
   - 0: Idle state
   - 1: Distributing Keys
   - 2: Re-encrypting Database

Note:

Each encryption key cycling job takes a minimum of 5 to 10 minutes to move to the next status. However, the process is delayed if there are offline Citrix Provisioning servers and servers waiting on key distribution.

Using McliPsSnapIn:

1. Open the **PowerShell** window.
2. Install the **PowerShell Snap-In**. The path where the `Citrix.PVS.SnapIn.dll` is installed is: `Import-Module "C:\Program Files\Citrix\Provisioning Services Console\McliPSSnapIn.dll"`
3. Run `Mcli-Run CycleEncryptionKeys` to start the key rotation process. After you run the command, the key rotation status changes to **Distributing Keys**.

> **Note:**
>
> If you run the command `Mcli-Run CycleEncryptionKeys` when the key rotation status is **Distributing Keys** or **Re-encrypting Database**, you get an error because the key rotation is in process and keys can be rotated only when the key rotation status is **Idle**.

4. Run `Mcli-Get PendingServers` to get the list of servers in the farm that are waiting on key distribution and servers that are offline.

> **Note:**
>
> - When the key rotation status is:
>   - **Distributing Keys**, you get the list of servers that are waiting on key distribution.
>   - **Re-encrypting Database** or **Idle**, you get the list of servers that are offline.
> - You might see a Citrix Provisioning server that initiated the key rotation in the list of servers that are waiting on key distribution even after the server in the farm gets the new encryption key immediately. Wait for approximately 5 minutes for that server to finish its key rotation process, after which it moves out of the list.

5. Turn on the servers that are offline. Ensure that the servers in the farm can communicate with the Citrix Cloud to get the encryption key.
6. After the key rotation process is complete, the status of the key rotation must change to **Idle**. Run the command `Mcli-Get Farm` to verify the key rotation status. The values of the property `EncryptionStatus`:
   - 0: Idle state
   - 1: Distributing Keys
   - 2: Re-encrypting Database

> **Note:**

> Each encryption key cycling job takes a minimum of 5 to 10 minutes to move to the next status. However, the process is delayed if there are offline Citrix Provisioning servers and servers waiting on key distribution.

Using the console to configure a farm

Run the Configuration Wizard on a provisioning server when creating a farm, adding new provisioning servers to an existing farm, or reconfiguring an existing provisioning server.

If all provisioning servers in the farm share configuration settings such as site and store information, consider Running the Configuration Wizard Silently.

Starting the configuration wizard

The Configuration Wizard starts automatically after Citrix Provisioning software is installed. The wizard can also be started by selecting **Start > All Programs > Citrix > Citrix Provisioning > Citrix Provisioning Configuration Wizard**.

Configuration wizard settings

Before running the Configuration Wizard, be prepared to make the following selections:

- Network topology
- Identify the farm
- Identify the database
- Create a store for a new farm
- Identify the site
- Join Citrix Cloud or Citrix Virtual Apps and Desktops site
- Select the license server
- Configure user account settings
- Select network addresses for the stream service
- Configure bootstrap Server
- Finish the configuration

> **Note:**

> If errors occur during processing, the log is written to a ConfigWizard.log file, which is at C:\ProgramData\Citrix\Citrix Provisioning.

> **Tip:**
>
> The Configuration Wizard was modified at release 7.12 to include support for Linux streaming. See the installation article for information about the Linux streaming component.

Network topology

Complete the network configuration steps that follow.

1. Select the network service to provide IP addresses

   Note: Use existing network services if possible. If existing network services cannot be used, choose to install the network services that are made available during the installation process.

   To provide IP addresses to target devices, select from the following network service options:

   - If the Dynamic Host Configuration Protocol (DHCP) service is on this server, select the radio button next to one of the following network services to use, then click **Next**:
     - Microsoft DHCP
     - Citrix Provisioning BOOTP service
     - Other BOOTP or DHCP service
   - If the DHCP service is not on this server, select the radio button next to **The service is running on another computer**, then click **Next**.

2. Select the network service to provide PXE boot information

   Each target device downloads a boot file from a TFTP server.

   Select the network service to provide target devices with PXE boot information:

   - If you use Citrix Provisioning to deliver PXE boot information, select **The service that runs on this computer**. Then select from either of the following options, then click **Next**:
     - Microsoft DHCP (options 66 and 67)
     - Citrix Provisioning PXE Service

- If Citrix Provisioning does not deliver PXE boot information, select **The information is provided by a service on another device** option, then click **Next**.

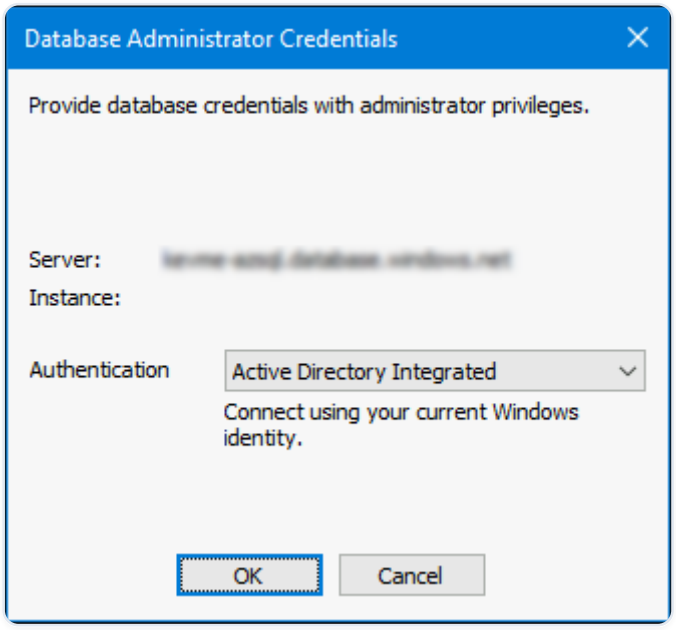
Identify the farm

1. Select from the following farm options:

   - Farm is already configured

     a. On the **Farm Configuration** dialog, select the option **Farm is already configured**, and click **Next**. This option appears only if a farm has been previously configured on this server.

     b. Enter database administrator credentials in the pop-up dialog. Select **Active Directory Integrated** authentication if you want to use the current login. Click **Ok**.



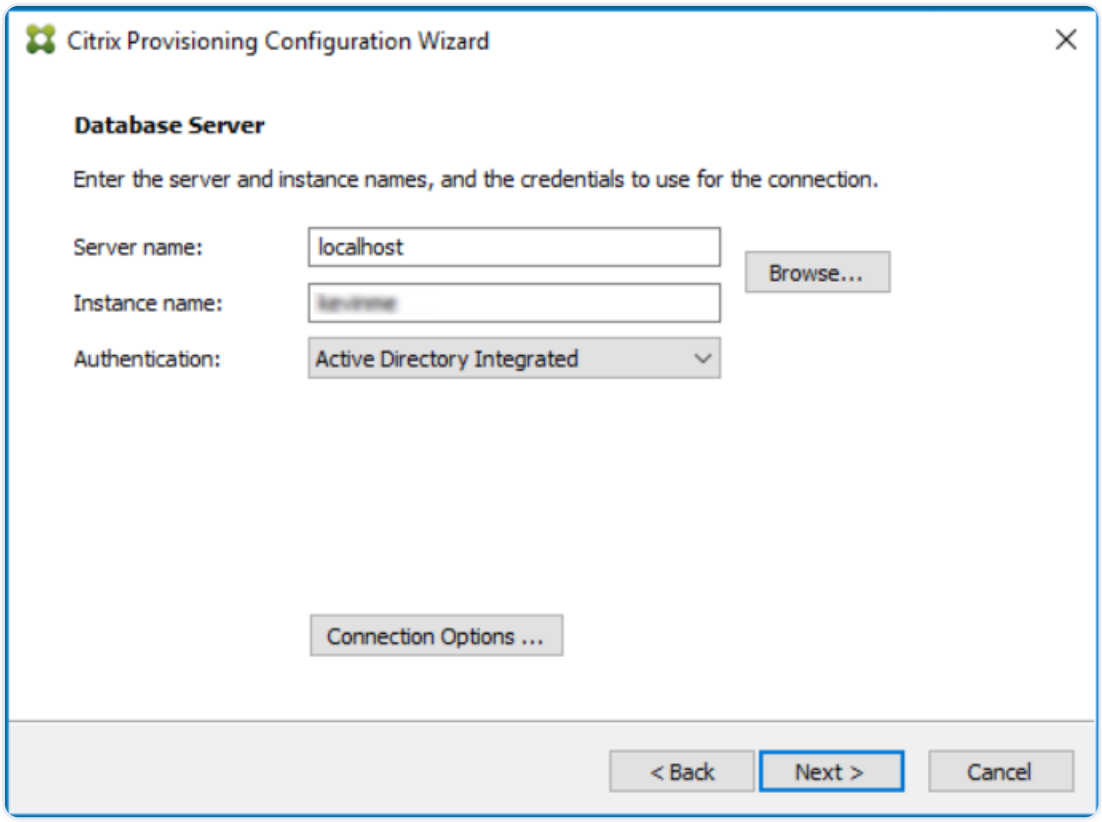
     c. Continue to the *Configure user account settings* procedure.

   - Create the farm

     a. On the **Farm Configuration** dialog, select the option **Create a Farm**, and click **Next**.

     b. On the **Databse Server** dialog,

        i. Use the **Browse** button to browse for existing SQL databases and instances in the network, or type the database server name and instance.



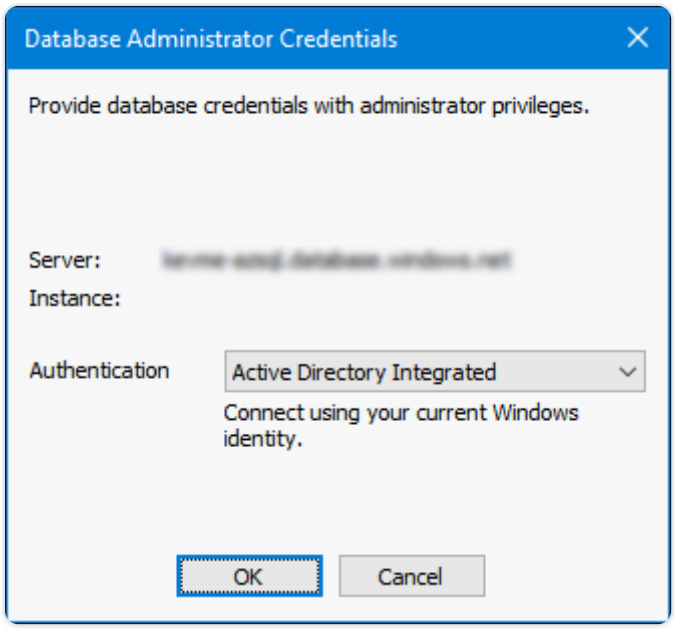
> **Note:**
>
> The combination of the database name and farm name must not exceed 54 characters. In such cases, the farm name displays as a truncated entry in the **Existing Farms** screen.

ii. To enable multi-subnet failover for SQL server, specify a database mirror failover partner, or enter a TCP port number, click **Connection Options ...**.

iii. Select **Active Directory Integrated** authentication if you want to use the services' user account. Enter the database credentials that the Stream and SOAP services will use.

iv. Click **Next**.

c. Enter database administrator credentials in the pop-up dialog. Select **Active Directory Integrated** authentication if you want to use the current login. Click **Ok**.



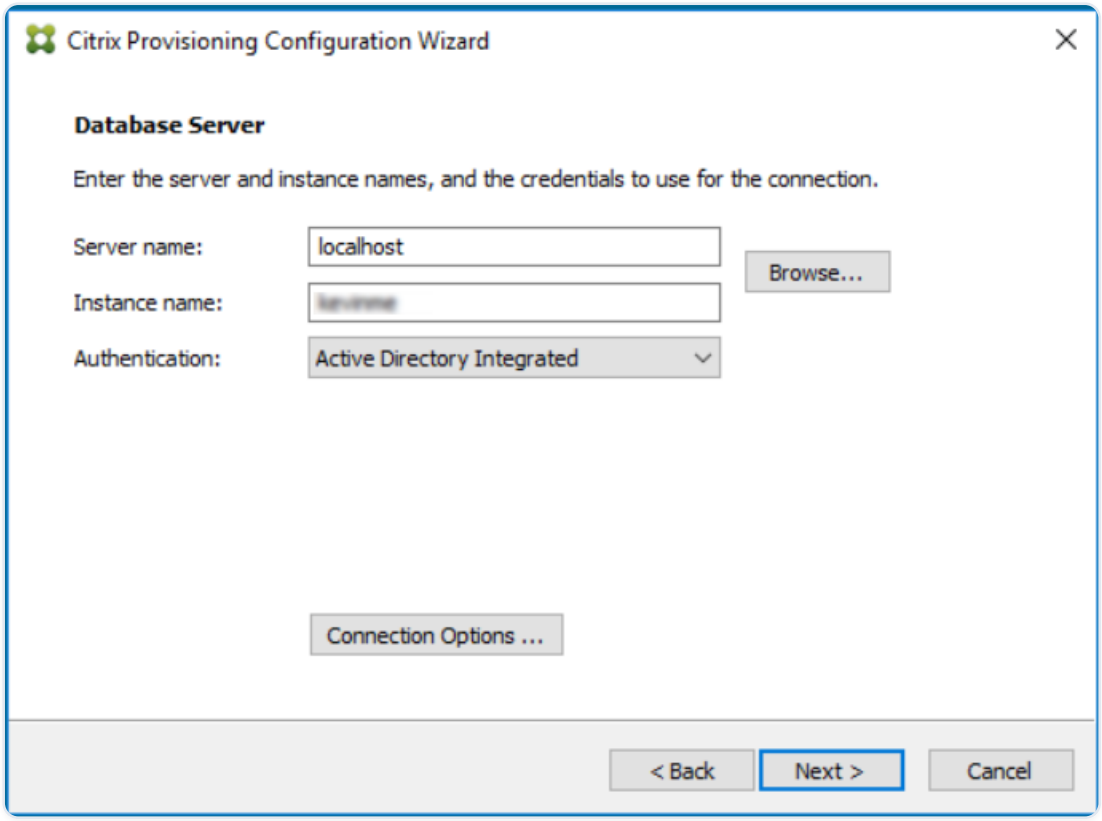
d. Select the database location.

- Join an existing farm

a. On the **Farm Configuration** dialog, select the option **Join Existing Farm** to add this provisioning server to an existing farm, then click **Next**.

b. On the **Databse Server** dialog:

i. Use the **Browse** button to browse for the appropriate SQL database and instance within the network.



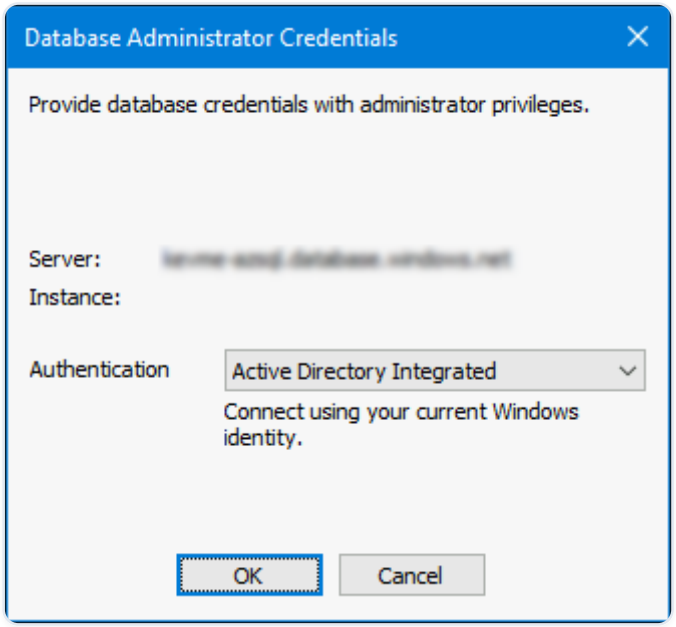
ii. Select the farm name that displays by default, or scroll to select the farm to join. Note: More than one farm can exist on a single server. This configuration is common in test implementations.

iii. To enable multi-subnet failover for SQL server, specify a database mirror failover partner, or enter a TCP port number, click **Connection Options ...**.

iv. Select **Active Directory Integrated** authentication if you want to use the services' user account. Enter the database credentials that the Stream and SOAP services will use.

v. Click **Next**.

c. Enter database administrator credentials in the pop-up dialog. Select **Active Directory Integrated** authentication if you want to use the current login. Click **Ok**.



d. Select from the following site options, then click **Next**:

- Existing Site: Select the site from the menu to join an existing site.
- New Site: Create a site by typing the name of the new site and a collection.

e. Continue on to configure the user account settings.

Identify the database

Only one database exists within a farm. To identify the database:

1. If the database server location and instance have not yet been selected, complete the following procedure.

a. On the **Database Server** dialog, click **Browse** to open the **SQL Servers** dialog.

b. From the list of SQL Servers, select the name of the server where this database exists. Specify the instance to use (to use the default instance, SQLEXPRESS, leave the instance name blank). In a test environment, this configuration can be a staged database. **Note:** Rerunning the Configuration Wizard to add extra provisioning server database entries, populates the **Server Name** and **Instance Name** text boxes. By default, SQL Server Express installs as an instance named *SQLEXPRESS*.

c. Select **Active Directory Integrated** authentication if you want to use the services' user account. Enter the database credentials that the Stream and SOAP services will use.

d. Click **Next**. If this database is a new farm, continue on to the *Defining a Farm* procedure.

2. To change the database to a new database

a. On the old database server, perform a backup of the database to a file.

b. On the new database server, restore the database from the backup file.

c. Run the Configuration Wizard on each Citrix Provisioning server.

d. Select **Join existing farm** on the **Farm Configuration** dialog.

e. Enter the new database server and instance on the **Database Server** dialog.

f. Select **Active Directory Integrated** authentication if you want to use the services' user account. Enter the database credentials that the Stream and SOAP services will use.

g. Select the restored database on the **Existing Farm** dialog.

h. Select the site that the provisioning server was previously a member of on the **Site** dialog.

i. Click **Next** until the Configuration Wizard finishes.

3. Define a farm. Select the security group to use:

- Use Active Directory groups for security **Note:** When selecting the Active Directory group to act as the farm administrator from the menu, choices include any group the current user belongs to. This list includes Built in groups, which are local to the current machine. Avoid using these groups as administrators, except for test environments. Some group names might be misleading and appear to be *domain groups*, but are *local domain groups*. For example, `ForestA.local/Builtin/Administrators`.
- Use Windows groups for security

4. Click **Next**.

Continue on to select the license server.

Create a store for a new farm

A new store can be created and assigned to the Citrix Provisioning server being configured:

Note: The Configuration Wizard only allows a server to create or join an existing store if it is new to the database. If a server exists in the database and it rejoins a farm, the Configuration Wizard might prompt the user to join a store or create a store. During this process, the selection is ignored.

1. On the **New Store** page, name the new Store.
2. Browse or enter the default path (for example: C:\\PVSStore) to use to access this store, then click **Next**. If an invalid path is selected, an error message appears. Reenter a valid path, then continue. The default write cache location for the store is located under the store path for example: C:\\PVSStore\\WriteCache.

Identify the site

When joining an existing farm, identify the site where this provisioning server is a member. Identify a site by either creating a site or selecting an existing site within the farm. When a site is created, a default target device collection is automatically created for that site.

Join Citrix Cloud or Citrix Virtual Apps and Desktops site

Using the **Join Citrix Cloud or CVAD** page, you can choose to join your farm with Citrix Cloud, a Citrix Virtual Apps and Desktops site, or choose to not join your farm.

> **Important:**
>
> - The **Join Citrix Cloud or CVAD** page appears only when the farm is NOT joined. If you select to join the farm to Citrix Cloud or Citrix Virtual Apps and Desktops site, you do not see this page again.
> - If you want to revert to a non-cloud joined or non-Citrix Virtual Apps and Desktops site joined farm, you must recreate the farm.

> If you choose to join your farm with Citrix Cloud, then you can additionally:

- Provision Citrix Provisioning targets using the DaaS Web Studio (Full Configuration interface).
- Have enhanced database encryption. For more information, see Encryption.

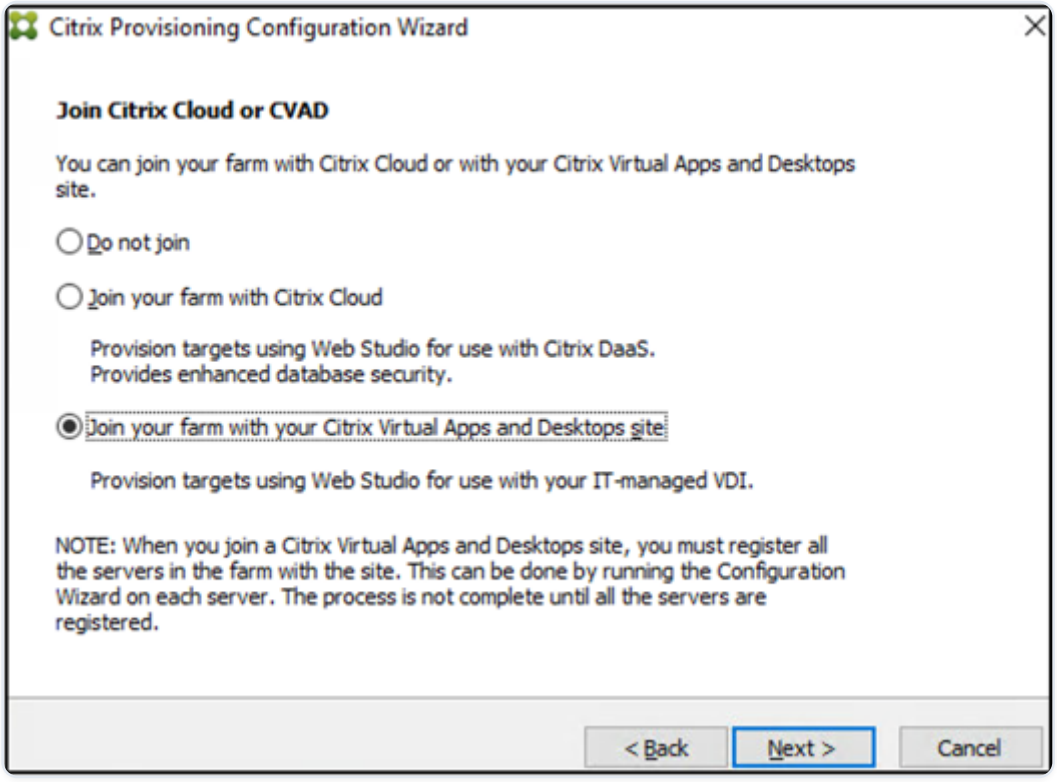
If you choose to join your farm to a Citrix Virtual Apps and Desktops site, then you can additionally:

- Provision Citrix Provisioning targets using the Citrix Virtual Apps and Desktops Web Studio.

Note:

- For successfully joining your farm to a Citrix Virtual Apps and Desktops site, when running the Configuration Wizard, use a Windows login that has Machine Catalog Administrator or higher privileges in Citrix Virtual Apps and Desktops.
- If you want to join your farm to a Citrix Virtual Apps and Desktops site, you must provision an SSL server certificate on all the servers in the farm. You can do this at a later step. See Creating self-signed certificates with PoSH.

1. On the **Join Citrix Cloud or CVAD** page, select one of the following:
   - **Do not join**
   - **Join your farm with Citrix Cloud**
   - **Join your farm with your Citrix Virtual Apps and Desktops site**



2. Click **Next**. If you choose to join your farm with Citrix Cloud or a Citrix Virtual Apps and Desktops site, then click **Yes** to confirm the action.

If you select to join your farm to Citrix Cloud or a Citrix Virtual Apps and Desktops site, see the required topics:

- If you select to join with Citrix Cloud
- If you select to join with a Citrix Virtual Apps and Desktops site

If you select to not join your farm, do the steps from Select the license server.

Note:

If you select to not join your farm, you see the **Join Citrix Cloud or CVAD** page every time you run the Configuration Wizard.

If you select to join with Citrix Cloud

If you select to join your farm with Citrix Cloud, follow these key steps:

1. Using the **Citrix Cloud Registration** page, register all the Citrix Provisioning Servers with Citrix Cloud. However, if a server is already registered and the registration is still valid, the page is skipped, and you directly go to the **Resource Location** page. If a server was previously registered, however, the registration has become invalid, then you are prompted to register again. For more information on how to register, see Register with Citrix Cloud.
2. Using the **Resource Location** page, select a resource location for the Citrix Provisioning target site. For more information on how to select the resource location, see Select a Resource Location.
3. Continue with the steps from Select the license server.

Register with Citrix Cloud

Once you select to join your farm with Citrix Cloud, every server needs to be registered. Registration allows all the Citrix Provisioning Servers to authenticate and communicate with Citrix Cloud without the need to log in to Citrix Cloud. To register, do the following:

On the **Citrix Cloud Registration** page, do the following:

1. Review the page. If this is the first server to register, the page indicates that no customer has been established for the farm yet. Otherwise, you can see the customer ID on the page that is registered with the servers in the farm.

> **Note:**
>
> All the servers in the farm must register with the same customer account

2. Click **Next** to start the registration with Citrix Cloud. A message appears indicating that the Configuration Wizard is registering.

On the **Confirm the Citrix Cloud Registration** dialog:

1. Follow the instructions as provided in the dialog to manually confirm the registration. This action requires you to log in to Citrix Cloud as account administrator.
2. After the registration is confirmed, the dialog automatically closes. Do not press **Cancel** unless you wish to abort the Configuration Wizard.

> **Note:**
>
> If for some reason, you delete an unregistered Citrix Provisioning server when all the other servers are registered, the farm's state is still considered partially joined. To resolve the issue, run the Configuration Wizard on any of the Citrix Provisioning servers that is joined to Citrix Cloud. Select the option **Farm is already configured**.

Select a Resource Location

On the **Resource Location** page:

1. Select a resource location for the Citrix Provisioning target site. You can also select **No resource location** from the options if:
    - you do not use DaaS Web Studio to provision Citrix Provisioning targets.
    - you use DaaS Web Studio to provision Citrix Provisioning targets, however, not for the specified Citrix Provisioning target site.

> **Note:**
>
> If a resource location has already been configured for the site, and you select a different resource location from the list, you get a confirmation pop-up after you click **Next**.

> Continue with the steps from Select the license server.

If you select to join with a Citrix Virtual Apps and Desktops site

If you select to join your farm with a Citrix Virtual Apps and Desktops site, you must select a Delivery Controller™ in the Citrix Virtual Apps and Desktops site that you want to join.

Key steps:

1. Using the **Citrix Virtual Desktops™ Controller** page, select a Delivery Controller. For more information, see Select a Delivery Controller.
2. Continue with the steps from Select the license server.

Select a Delivery Controller

You must select a Delivery Controller in the Citrix Virtual Apps and Desktops site that you want to join.

On the **Citrix Virtual Desktops Controller** page:

1. Review the page. If this is the first server to register, the page indicates that no Citrix Virtual Apps and Desktops site has joined the farm yet. In that case, select a Delivery Controller to establish the Citrix Virtual Apps and Desktops site that the farm will join. If this is not the first server to register, you can see the name of the Citrix Virtual Apps and Desktops site with which servers in the farm are registered.

   > **Note:**
   >
   > All the servers in the farm must connect to the same Citrix Virtual Apps and Desktops site.

2. Click **Next**. The controller address is validated. You get an authorization error if you are not using a Windows login that has Machine Catalog Administrator or higher privileges on the Citrix Virtual Apps and Desktops site.

Continue with the steps from Select the license server.

Select the license server

1. Enter the fully-qualified domain name of the license server, a hostname, or an IP address if that is supported by the license server.

2. Enter the port number of **License Server Port** and **Web Services for Licensing Port**.

   Default value of Licensing Server Port is 27000.

   Default value of Web Services for Licensing Port is 8083.

   The provisioning server must be able to communicate with both the licensing server port and web services for licensing port on the license server to get the appropriate product licenses.

3. The checkbox **Validate license server communication** is selected by default. This option verifies that the server can communicate with the license server and that the appropriate version of the license server is used. If the server is not able to communicate with the license server, or the wrong version of the license server is being used, an error message appears. You cannot proceed.

4. Select the license to be used.

   > **Note:**
   >
   > - If you have a DaaS (Citrix Cloud) license, then select **Citrix Cloud**.
   > - If you have an on-premises Citrix Virtual Apps and Desktops license or are operating independently of Citrix Virtual Apps and Desktops, then select **Citrix Virtual Apps and Desktops**.

5. Click **Next** to continue on to configure user account settings.

Configure user account settings

The Stream and Soap services run under a user account. Configure data reader and data writer database roles automatically using the Configuration Wizard to provide database access privileges to a user account.

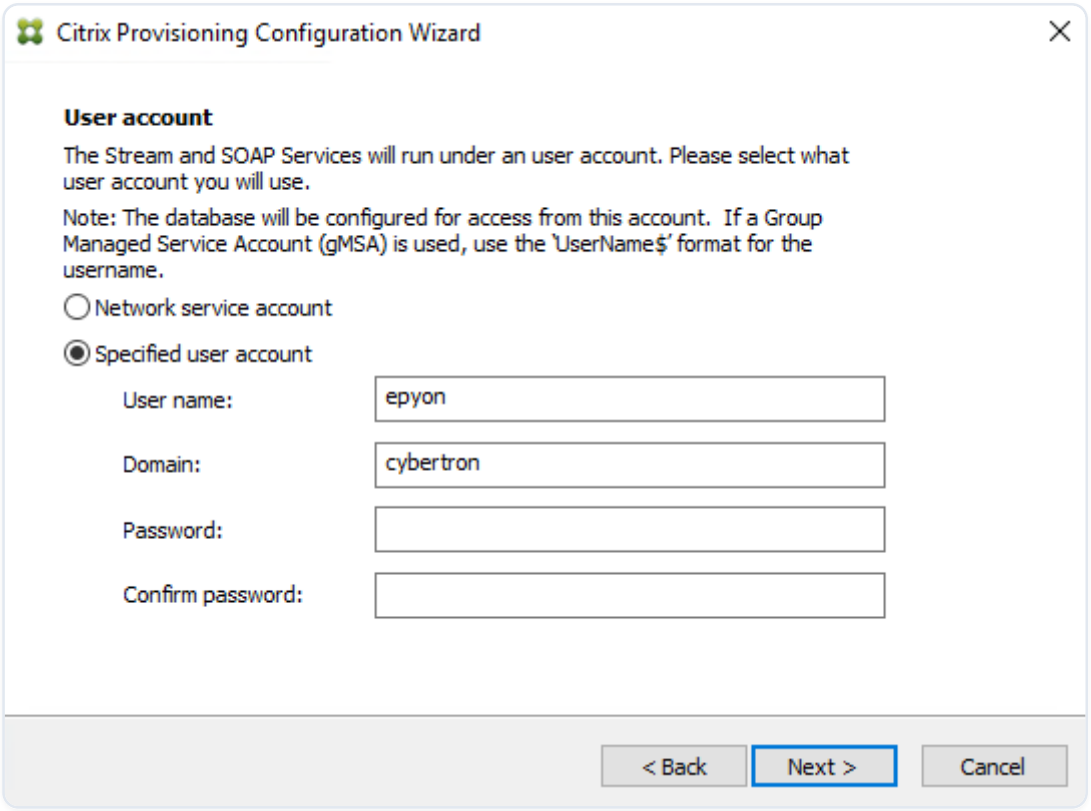
1. On the **User Account** dialog, select the user account that the Stream and Soap services run under:

   - Network service account (minimum privilege local account that authenticates on the network as computers domain machine account).
   - Specified user account (required when using a Windows **Share**; workgroup or domain user account). Type the user name, domain, and password information in the appropriate text boxes.

2. Click **Next**, then continue on to selecting network cards for the Stream Service.

Group managed service accounts

Citrix Provisioning supports Group Managed Service Accounts (gMSA). These accounts are managed domain accounts providing automatic password management and simplified SPN management over multiple servers.



Deploy certificates

You must select a certificate for all the servers in the farm if you want to:

- Join your farm to a Citrix Virtual Apps and Desktops site
- Use the Imaging Wizard for Linux targets
- Provision targets using the Citrix Provisioning API

Use the Citrix Provisioning Configuration Wizard to add the proper certificate from the local Computer personal certificates (**My**) store.

> **Note:**
>
> We recommend to use a CA-signed certificate but you can use a self-signed certificate if necessary.

For deploying a certificate:

1. Import the certificate into `My` store on the Citrix Provisioning server.
2. Install the root of trust of the certificate in the trusted root store of the client machines where connections are made (PVSAPI, Linux machine that is imaged and Citrix Virtual Apps and Desktops Delivery Controller).

Note:

The set of operations depends on whether you use a CA-signed certificate or self-signed certificate.

1. Run the Configuration Wizard. On the **SSL Configuration** page, select the certificate to use.

Use a CA-signed certificate

The CA-signed certificate must include both public and private key and the private key must be exportable.

1. Import the certificate into `My` store on the Citrix Provisioning server.

```
Import-Certificate -FilePath <crt file> -CertStoreLocation Cert:
\LocalMachine\My
```

2. If the certificate authority root certificate is not in the trusted root store (`Cert:\LocalMachine\Root`) on every client machine, then add it on all client machines. However, this step is usually not required when using a public CA-signed certificate.

Use a self-signed certificate

1. Create a self-signed certificate.

```
$cert = New-SelfSignedCertificate -DnsName $PVS_SERVER_FQDN
-CertStoreLocation cert:\LocalMachine\My

$cert_thumbprint = $cert.Thumbprint
```

> **Note:**
>
> When you create a certificate, you can specify multiple `-DnsName`, separated by a comma. This adds Subject Alternative Names to the certificate, one for each `DnsName`. When using the PVS API, you can connect using any of these names. Example: You can use -DnsName "servername.domain", "servername". Then, using PVS API connect with -PvsServerAddress "servername.domain" or -PvsServerAddress "servername".

2. Export the certificate to the `.cer` file without its private key.

```
Export-Certificate -Cert $cert -FilePath $CERT_FILE
```

3. On each client machine, import the exported self-signed into the `Cert:\LocalMachine\Root` trusted root store on the client.

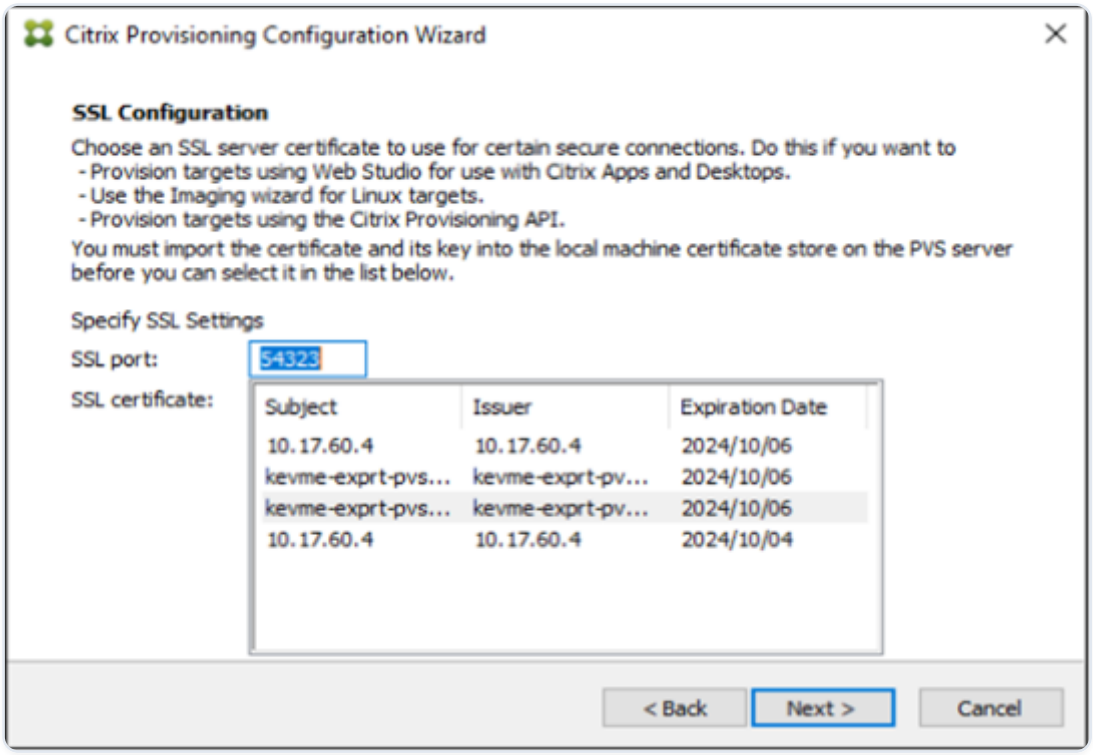
```
$file = ( Get-ChildItem -Path $CERT_FILE )

$file | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root
```

Use Configuration Wizard to deploy certificate

Use the Citrix Provisioning Configuration Wizard to add the proper certificate from the local Computer personal certificates (**My**) store.

The **SSL Configuration** page displays the certificate that is imported into **My** store on the Citrix Provisioning Server.



Tip:

When the **Soap SSL Configuration** page first loads, the certificate is highlighted which gives the appearance that it is selected. Ensure that the certificate is selected, it appears as a blue item in the table.

Select network addresses for the stream service

1. Select the checkbox next to each of the network addresses that the Stream Service can use. Both IPv4 and IPv6 addresses that are assigned to the Citrix Provisioning Server are displayed. You can proceed with one of the following combinations:

   - Only IPv4 address
   - Only IPv6 address
   - Combination of both IPv4 and IPv6 address

2. Enter the base port number that is used for network communications in the First communications port: text box.

   Note:

> A minimum of 20 ports are required within the range. All provisioning servers within a farm must use the same port assignments.

3. Select the Soap Server port (default is 54321) to use for Console access, then click **Next**.

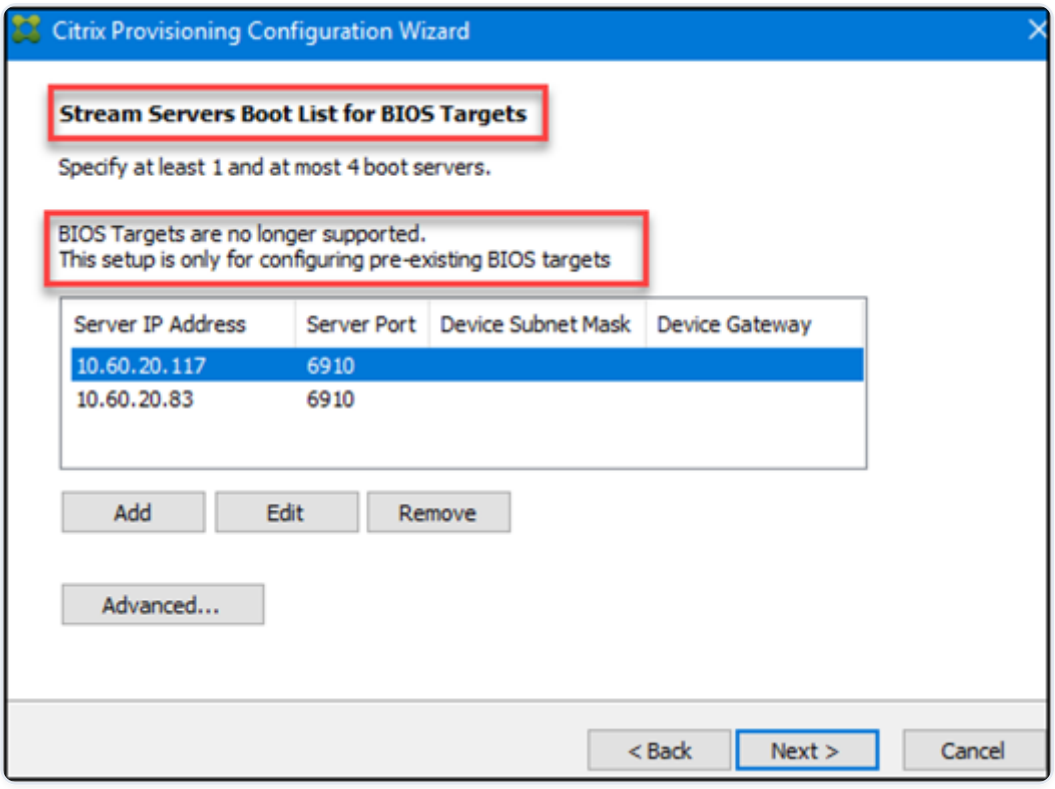
Continue on to select the bootstrap server.

Configure the bootstrap server

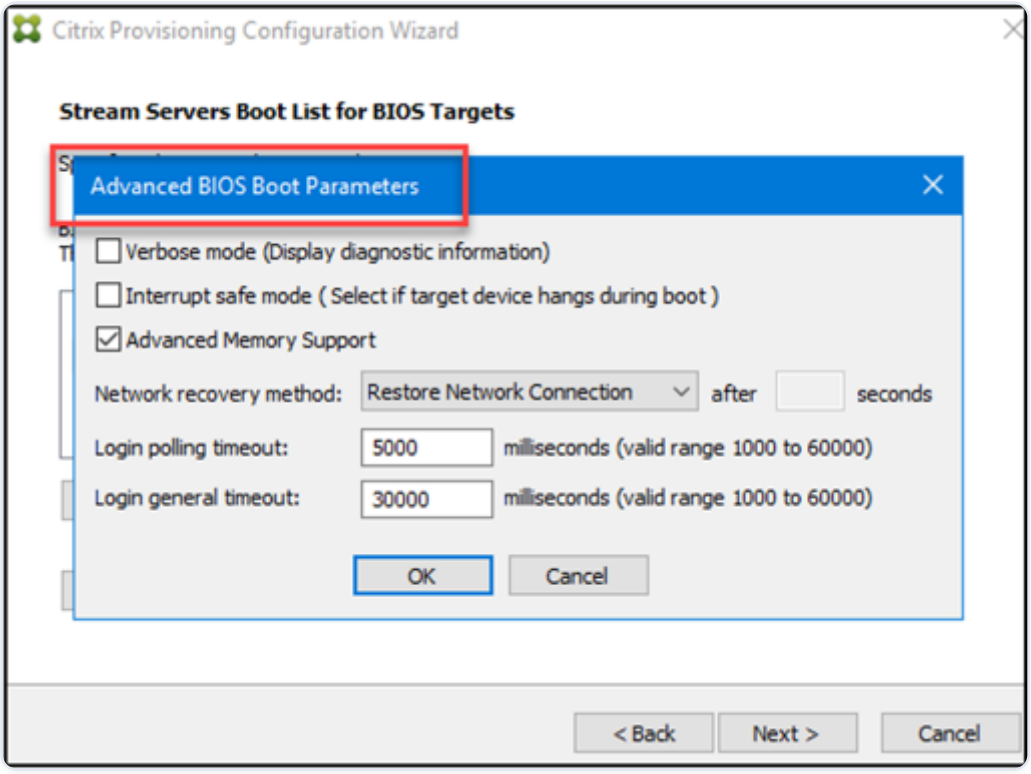
> **Note:**
>
> BIOS targets are no longer supported. These instructions are only for configuring pre-existing BIOS targets.

1. Select **Provisioning Servers** to use for the boot process:

   a. Use the **Add** button to add more provisioning servers to the list. The **Edit** button to edit existing information, or to remove the server from the list. Use the **Move up** or **Move down** buttons to change the server boot preference order. The maximum length for the server name is 15 characters. Do not enter the **FQDN** for the server name. In a high availability implementation, at least two provisioning servers must be selected as boot servers.



b. Optionally, highlight the IP address of the provisioning server that target devices boot from, then click **Advanced**. The **Advanced Stream Servers Boot List** appears.



The following list describes advanced settings that you can choose from. After making your selections, click **OK** to exit the dialog, then click **Next** to continue.

- **Verbose mode:** Select the Verbose Mode option if you want to monitor the boot process on the target device (optional) or view system messages.
- **Interrupt safe mode:** Select **Interrupt Safe Mode** if you are having trouble with your target device failing early in the boot process. This option enables debugging of target device drivers that exhibit timing or boot behavior problems.
- **Advanced memory support:** This setting enables the bootstrap to support newer Windows OS versions and is enabled by default. Disable this setting on Windows Server OS 32 bit versions that do not support PXE. Or if your target device is hanging or behaving erratically in early boot phase.
- **Network recovery method:**
  - **Restore Network Connections:** Selecting this option results in the target device attempting indefinitely to restore its connection to the provisioning server.

> **Note:**

> Because the **Seconds** field does not apply, it becomes inactive when selecting the **Restore Network Connections** option.

    - **Reboot to Hard Drive:** (A hard drive must exist on the target device). Selecting this option instructs the target device to perform a hardware reset to force a reboot after failing to re-establish communications for a defined number of seconds. The user determines the number of seconds to wait before rebooting. Assuming the network connection cannot be established, PXE fails, and the system reboots to the local hard drive. The default number of seconds is 50, to be compatible with high availability configurations.

- **Logon polling timeout:** Enter the time in milliseconds between retries when polling for provisioning servers. Each server is sent a login request packet in sequence. The first responding server is used. In non-HA configurations, this time-out simply defines how often to retry the single available server with the initial login request. This time-out defines how quickly the round-robin routine switches from one server to the next in trying to find an active server. The valid range is from 1,000 milliseconds to 60,000 milliseconds.
- **Log in general timeout:** Enter the time-out in milliseconds for all login associated packets, except the initial login polling time-out. The time-out is longer than the polling time-out because the server needs time to contact all associated servers, some of which are unreachable. Unreachable servers require retries and time-outs from the provisioning server to the other provisioning servers to determine if they online. The valid range is from 1,000 milliseconds to 60,000 milliseconds.

2. Verify that all configuration settings are correct, then click **OK**.

Finish the configuration

On the **Finish** page, additional data about server registration is presented in the **Summary** section.

1. Run the Configuration Wizard to configure all the servers in the farm.
2. Click **Done** on the Finish page after configuration is complete.

Verify Citrix Provisioning server registration

To verify the Citrix Provisioning server registration:

1. Log in to `<customer>.cloud.com`.

2. Go to **Identity and Access Management > API Access > Product Registrations**. You can see the current registrations.

Restore database

You can restore the database from a backup when using enhanced database encryption if you rotate the keys between taking the backup and restoring the database.

> **Note:**
>
> - The enhanced encryption is available only after you join a farm to the Citrix Cloud.
> - The database encryption key is synchronized between Citrix Cloud, Citrix Provisioning Server's registry, and database every 24 hours.

To restore the database when using enhanced encryption:

1. Take a backup of the database using **SQL Server Management Studio** when the key rotation state is **Idle**.
2. Restore the database.
    a. Wait for the key rotation state to be **Idle** if a key rotation is in progress.
    b. Stop all Citrix Provisioning Services on all Citrix Provisioning Servers in the farm - SOAP, stream process, and Citrix Provisioning API. This action ensures that all active connections to the database are closed.
    c. Restore the database using **SQL Server Management Studio**.
3. Get the Citrix Provisioning Servers online.
    a. Run the Configuration Wizard on all the servers in the farm. After you click **Finish**, the system displays a prompt to indicate that the database has been restored and key rotation is required. Click **OK**.
4. Rotate the key using one of the following:
    - Go to the **Citrix Provisioning Console > Farm > Properties > Encryption** tab. For more information, see Encryption tab.

        > **Note:**

> After you launch the Citrix Provisioning Console, the farm icon is replaced with a warning icon. The **General**, **Encryption**, and **Status** tabs of **Farm > Properties** also display a warning message to indicate that the database has been restored and key rotation is required. The warning icon and the message disappear after you rotate the key.

- Use the PowerShell command `Start-PvsRotateEncryptionKeys`. For more information, see Using PowerShell and MCLI commands to rotate encryption key.

Server

You typically perform the following tasks when configuring Citrix Provisioning™ servers in your farm.

> **Important:**
>
> After changing a provisioning server's properties, restart the Stream Service to implement those changes. Use caution when restarting services. If target devices are connected to the server, changes can prevent the device from reconnecting. The **IP address** field on the **Network** tab must reflect the real static IP address of the server.

> **Note:**
>
> A single provisioning server supports up to 4,095 target devices.

Provisioning server properties

On the Citrix Provisioning console, the **Server Properties** dialog allows you to modify provisioning server configuration settings.

> **Note:**
>
> Avoid modifying any of the settings if the current settings are working without any issues.

To view existing properties, choose one of the following methods:

- Highlight a provisioning server, then select **Properties** from the **Action** menu.
- Right-click a provisioning server, then select **Properties**.
- If the details pane is open, highlight a provisioning server, then select the **Properties** menu item from the list of actions.

The **Server Properties** dialog includes the following tabs:

- General
- Network
- Stores
- Options
- Logging

Tip:

Citrix Provisioning displays a message when a change made on a **Server Properties** dialog requires a server reboot.

General tab

FIELD	DESCRIPTION
Name and description	Displays the name of the provisioning server and a brief description. The maximum length for the server name is 15 characters. Do not enter **FQDN** for the server name.
Power rating	A power rating is assigned to each server, which is then used when determining which server is least busy. The administrator defines the scale to use. For example, an administrator rates all servers on a scale of 1–10, or on a scale of 100–1000. On a scale of 1–10, a server with a rating of 2 is considered twice as powerful as a server with a rating of 1. Therefore it would be assigned twice as many

FIELD	DESCRIPTION
	target devices. When using a scale of 100–1000, a server with a power rating of 200 is considered twice as powerful as a server with the rating of 100. Therefore it would also be assigned twice as many target devices. Using the default setting of 1.0 for all servers results in even device loading across servers. In this case, the load balancing algorithm does not account for individual server power. Ratings can range between 0.1-1000.0. 1.0 is the default.
Log events to the server's event log	Select this option if you want this provisioning server's events captured in the Windows Event log.
(Only if you join your farm with Citrix Cloud™) Citrix Cloud Registration	Displays the status of the server registration with Citrix Cloud and the validity of the server registration key.
(Only if you join your farm with a Citrix Virtual Apps and Desktops™ site) CVAD Site Registration	Displays the status of the server registration with a Citrix Virtual Apps and Desktops site.

Server tab

The following options are assessable in the **Advanced Server Properties** window.

FIELD	DESCRIPTION
Threads per port	Number of threads in the thread pool that service UDP packets received on a given UDP port. Between four and eight are reasonable settings. Larger numbers of threads allow more target device requests to be processed simultaneously, but consumes more system resources.
Buffers per thread	Number of packet buffers allocated for every thread in a thread pool. Make the number of buffers per thread large enough to enable a

FIELD	DESCRIPTION
	single thread to read one I/O transaction from a target device. Buffers per thread are ideally be set to `IOBurstSize / MaximumTransmissionUnit + 1`. Setting the value too large consumes extra memory, but does not hurt efficiency. Setting the value too small consumes less RAM, but detrimentally affects efficiency.
Server cache timeout	Every server writes status information periodically to the Citrix Provisioning database. This status information is time-stamped on every write. A server is accessible by other servers in the farm if the status information in the database is newer than the server cache timeout seconds. Every server in the farm attempts to write its status information every 2 seconds, at twice the timeout rate. A shorter server cache timeout value allows servers to detect offline servers more quickly, at the cost of extra database processing. A longer Server cache timeout period reduces database load at the cost of a longer period to detect lost servers.
Local and concurrent I/O limits	Controls the number of concurrent outstanding I/O transactions that can be sent to a given storage device. A storage device is defined as either a local drive letter (C: or D: for example) or as the base of a UNC path, for example \ServerName. Since Citrix Provisioning is a highly multi-threaded service, it is possible for it to send hundreds of simultaneous I/O requests to a given storage device. Requests are generated by the device and processed when time permits. Some storage devices, Windows Network Shares most notably, do not deal with this large number of concurrent requests well. They can drop connections, or take unrealistically long to process transactions in certain circumstances. You achieve better

FIELD	DESCRIPTION
	performance with these types of devices when you throttle the concurrent I/O transactions. A local device is defined as any device starting with a drive letter. A remote device is defined as any device starting with a UNC server name. Defining a device is a simple way to achieve separate limits for network shares and for local drives. If a slow machine provides a network share, or slow drives exist on the machine, a count of 1–3 for the remote limit is necessary. This configuration achieves the best performance with the share. If you are using fast local drives, you might be able to set the local count fairly high. Only empirical testing would provide you with the optimum setting for a given hardware environment. Setting either count to 0 disables the feature and allows Citrix Provisioning to run without limits. This configuration might be desirable on fast local drives. If a network share is overloaded, more device retries and reconnections during boot storms occurs. Boot storms occur when read/write and open file times are greater than 60 seconds. Throttling the concurrent I/O transactions on the share reduces these types of problems considerably.

Network tab

FIELD	DESCRIPTION
Maximum transmission unit	Number of bytes that fit in a single UDP packet. For standard Ethernet, the default value is correct. If you are attempting to operate over a WAN, then a smaller value is needed to prevent IP fragmentation. Citrix Provisioning does not currently support IP fragmentation and reassembly. If you are using a device or software layer that adds bytes to every packet for security reasons, a smaller value is needed. If your entire infrastructure

FIELD	DESCRIPTION
	supports jumbo packets you can set the MTU to 50 bytes less than your jumbo packet max size to achieve much higher network throughput.
I/O burst size	The number of bytes transmitted in a single read/write transaction before an ACK is sent from the server or device. The larger the I/O burst, the faster the throughput to an individual device, but the more stress placed on the server and network infrastructure. Also, larger I/O Bursts increase the likelihood of lost packets and costly retries. Smaller I/O bursts reduce single client network throughput, but also reduce server load. Smaller I/O bursts also reduce the likelihood of retries. I/O Burst Size / MTU size must be <= 32, that is, only 32 packets can be in a single I/O burst before an ACK is needed.
Socket communications	Enable non-blocking I/O for network communications.

Pacing tab

FIELD	DESCRIPTION
Boot pause records	The amount of time that the device pauses if the Maximum devices booting limit has been reached. The device displays a message to the user and then waits before attempting to continue to boot. The device continues to check with the server every Boot pause seconds until the server allows the device to boot.
Maximum boot time	The amount of time a device is considered in the booting state. Once a device starts to boot, the device is considered booting until the Maximum boot time has elapsed for that device. After this period, it will no longer be

FIELD	DESCRIPTION
	considered booting even if the device has not finished booting. Maximum boot time is the time limit per device for the booting state for boot pacing.
Maximum devices booting	The maximum number of devices a server boots at one time before pausing new booting devices. The number of booting devices must drop below this limit before the server allows more devices to boot.
Virtual disk creation pacing	Amount of pacing delay to introduce when creating a virtual disk on this provisioning server. Larger values increase the virtual disk creation time, but reduce provisioning server overhead to allow target devices that are running, to continue to run efficiently.

Device tab

FIELD	DESCRIPTION
License timeout	Amount of time since last hearing from a target device to hold a license before releasing it for use by another target device. If a target device shuts down abnormally (loses power for example) its license is held for the specified timeout period.

Network tab

FIELD	DESCRIPTION
IP address	The IP addresses that the stream service uses for a target device to communicate with this provisioning server. When you add a new server, enter the valid IP address for the new server. The following fields are including when viewing IP address information: **Add** — Add an IPv4 or IPv6 address for the selected server. **Edit** — Opens the **IP address** dialog so that

FIELD	DESCRIPTION
	the IP address for the selected server can be changed. **Remove** — Removes the selected IP address from the list of available IP addresses for the selected provisioning server.
Ports	Enter the **First and Last UDP port numbers** to indicate a range of ports to be used by the Stream Service for target device communications. **Note:** The minimum is five ports in a range. The default first port number is 6910 and the last port number is 6930.

Supported IP address

Citrix Provisioning supports the following streaming IP addresses:

- IPv4
- IPv6

Stores tab

FIELD	DESCRIPTION
Stores	Lists all stores (logical names representing physical paths to vDisks that are available to this provisioning server. This field includes the following options: **Add** — Opens the **Store Properties** dialog. A new store and that store's properties are included in the list of stores, overriding the default path. **Edit** — Opens the **Store Properties** dialog so that the store's properties can be changed. Select an existing store, then click **Edit** to change that store's properties. **Remove** — Removes the selected store from the list of available stores for this provisioning server.
Store properties	Includes the following fields: **Store** — The name of the store. This field displays when editing an existing store. For a new store, select the store from the menu. **Path** used to

FIELD	DESCRIPTION
	access the store — The store path is only required if you need to override the ‘default path’ configured in the store properties. If the default path in the store properties is valid for this server, leave the path for the store blank in the server store properties. **Note**: If you are setting an override store path in the Server's **Properties** dialog, set the path before creating a version of the virtual disk. Because this path information is stored and referenced in `.vhdx` header information, changing the path after versioning possibly causes unexpected results. **Write cache paths** — Click the **Add** or **Edit** buttons to open the **Write cache path** dialog, then enter the appropriate write cache path for this store. Select an existing path from the list, then click **Remove** to remove the paths association with the store. Use the **Move Up** and **Move Down** buttons to change the order of cache path priority. If configured for high availability, the order that the cache paths are listed must be the same order for each server.

Options tab

FIELD	DESCRIPTION
Active directory	Automate computer account password updates — If target devices are domain members, and require renegotiation of machine passwords between Windows Active Directory and the target devices, select the **Automate computer account password updates**. Use the slider to set the number of days between renegotiation.
Enable automatic virtual disk updates	Check to enable vDisks to update automatically, then set the time of day to check for updates.

Logging tab

FIELD	DESCRIPTION
Logging level	Select from the following logging level options: **TRACE** — TRACE logs all valid operations. **DEBUG** — The DEBUG level logs details related to a specific operation and is the highest level of logging. If logging is set to DEBUG, all other levels of logging information are displayed in the log file; **INFO** — Default logging level. The INFO level logs information about workflow, which generally explains how operations occur. **WARN** — The WARNING level logs information about an operation that completes successfully, but there are issues with the operation. **ERROR** — The ERROR level logs information about an operation that produces an error condition. **FATAL** — The FATAL level logs information about an operation that the system cannot recover from.
File size maximum	Enter the maximum size that a log file can reach before a new file is created.
Backup files maximum	Enter the maximum number of backup log files to retain. When this number is reached, the oldest log file is automatically deleted.

Copying and pasting properties

To copy the properties of one provisioning server to another provisioning server:

1. Right-click on the provisioning server to copy properties from, then select **Copy server properties**. The **Copy Server Properties** dialog appears.
2. Enable the check box next to each property to copy, or click the **Select all** button to copy all properties.
3. Click **Copy**. Right-click on the provisioning server that you want to copy properties to, then select **Paste**.

Configuring Citrix Provisioning servers manually

If you are setting up a remote provisioning server, or have special requirements, configure, and start your stream services manually. Run the Configuration Wizard on remote provisioning servers to insure that all settings are configured properly. Failure to run the Configuration Wizard makes it impossible for you to map a virtual disk.

Rerunning the configuration wizard

The Configuration Wizard can be used when updating the Stream Service of the IP address of your provisioning server changes. If you change your provisioning server's IP address for any reason, rerun the configuration wizard and choose the new IP address when prompted. Completing the Configuration Wizard resets the appropriate IP addresses in the configuration and restarts the Stream Service.

Starting and configuring the stream service manually

After configuring the Stream Service, you must start the service for the change to take effect. Citrix® recommends setting the service to start automatically each time a provisioning server starts.

> **Note:**
>
> The Configuration Wizard starts and configures the necessary services to start automatically. Use the instructions in this section. If you need to start and configure the services manually.

> Start the Stream Service for the provisioning server to operate. Start the following boot services if they have not yet been started:

- BOOTP Service or PXE Service
- TFTP Service

To manually start services:

1. From the **Windows Start** menu, select **Settings**, and then click **Control Panel**.
2. From the **Control** Panel, double-click the **Administrative Tools** icon.
3. From the Administrative Tools window double-click on the **Services** icon. The **Services** window appears.
4. From the **Services** window, right-click on the service you want to start, then select **Start**.

To manually configure services to start automatically upon booting the provisioning server:

1. From the **Windows Start** menu, select **Settings**, then click **Control Panel**.
2. From the **Control** Panel, double-click the **Administrative Tools** icon.
3. From the Administrative Tools window double-click on the **Services** icon. The **Services** window appears.
4. Right-click the service you want to configure, then select **Properties**.
5. Change the **Startup Type** to **Automatic** to configure the service to start automatically each time the system boots.

Deleting a provisioning server

Occasionally, you have to delete a provisioning server from the list of available servers in a farm.

> **Note:**
>
> Before you can delete a provisioning server, first mark the server as down or take the server off line, otherwise the **Delete** menu option fails to appear. The stream service cannot be deleted.

> When you delete a provisioning server, you do not affect virtual disk image files or the contents of the server drives. However, you do lose all paths to the virtual disk image files on that server.

After you delete a server, target devices are no longer assigned to any virtual disk image files on that server. The target device records remain stored in the Virtual LAN Drive database, but the device cannot access any virtual disk that was associated with the deleted server.

> **Note:**
>
> If there are vDisks associated with the provisioning server being deleted, Citrix recommends that you create backup copies and store them in the virtual disk directory before deleting.

> **To delete a provisioning server:**

1. In the Citrix Provisioning console, highlight the provisioning server that you want to delete, then select **Show connected devices** from the **Action** menu, right-click menu, or **Action** pane. The **Connected Target Devices** dialog appears.
2. In the **Target Device** table, highlight all devices in the list, then click **Shutdown**. The **Target Device Control** dialog appears.
3. Type a message to notify target devices that the provisioning server is being shut down.
4. Scroll to select the number of seconds to delay after the message is received.
5. If the Stream Service is running on the provisioning server, stop the Stream Service. For more information, see Starting, Restarting, or Stopping the Stream Service.
6. Unassign all target devices from the provisioning server.
7. Highlight the server you want to delete, then choose **Delete** from the **Action** menu, right-click menu, or **Action** pane. A delete confirmation message appears.
8. Click **Yes** to confirm the deletion. The provisioning server is deleted and no longer displays in the console.

To decommission a provisioning server:

1. Verify if any provisioned clients are owned by the provisioning server you want to remove. If a provisioned client exists, shut it down.
2. If provisioned clients are owned by multiple servers, stop the stream service.
3. In the Citrix Provisioning console on the remaining provisioned server, the server appears as down, or, offline. Select the server, right click, and select **Delete** in the contextual menu.
4. Shut down the system or uninstall the provisioning server.

Starting, stopping, or restarting a server

> **Tip:**
>
> Starting, stopping, or restarting Citrix Provisioning can possibly result in unexpected behavior. For more information, see Servers.

> **To start, stop, or restart Citrix Provisioning Services on a provisioning server:**

1. Highlight the provisioning server in the Console, then select the **Stream Services** menu option from the **Actions** menu, right-click menu, or **Actions** pane. The **Server** dialog appears.

2. Select from the following menu options:
3. Highlight the provisioning servers that you want to configure, then click that action's button.
4. Click **Close** to exit the dialog.

FIELD	DESCRIPTION
Start	Starts the Stream Service
Stop	Places the provisioning server in off-line mode
Restart	After modifying provisioning server settings, such as adding or removing IPs, restart the stream service.

Important considerations

To start or stop SOAP or stream services on a provisioning server, you must have Windows permissions. This limitation is due to a Window's security issue.

To resolve this issue, use `icacls` to set the permissions on the Stream Service. See icacls for more information on `icacls`.

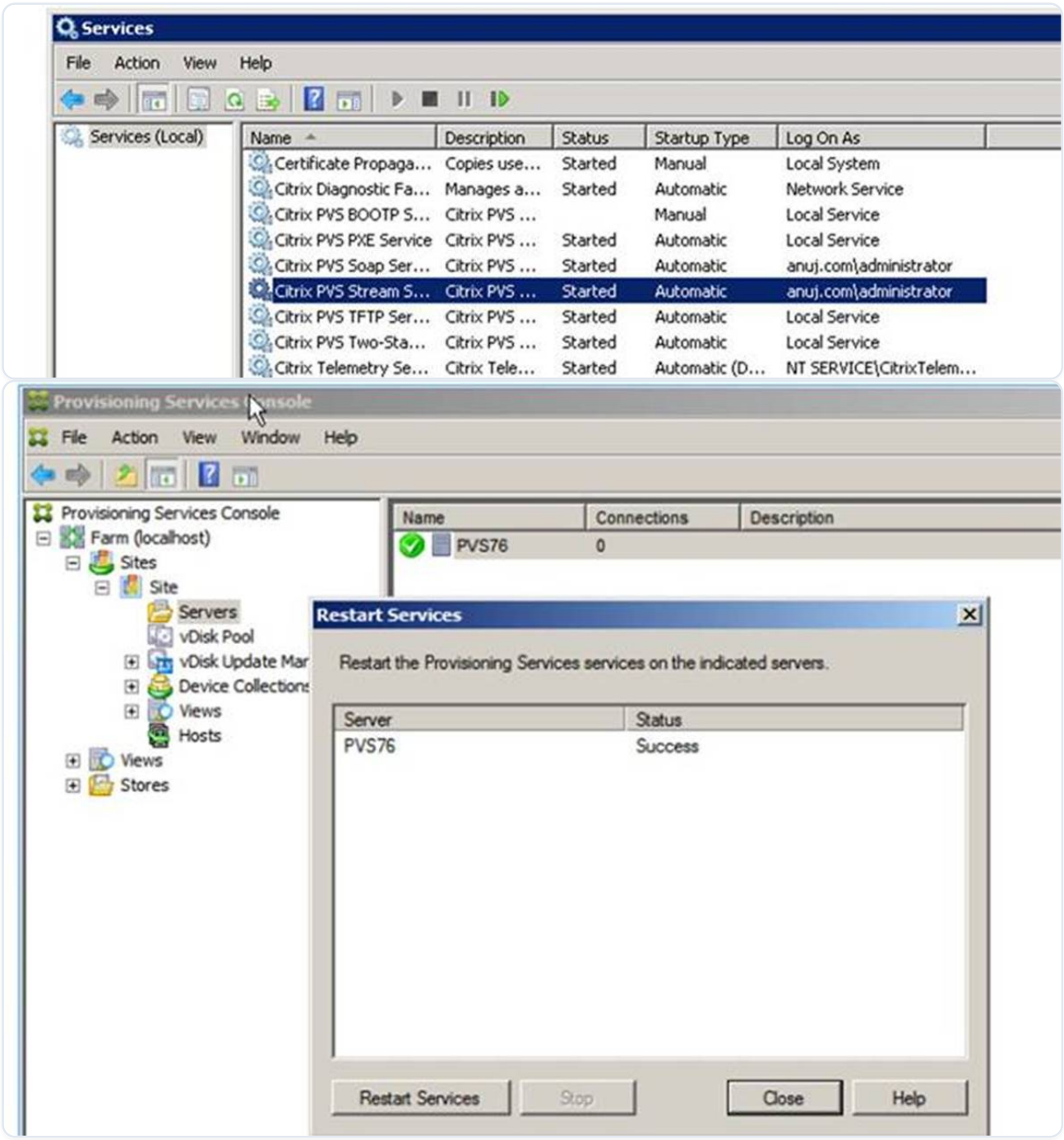
Citrix Provisioning console fails to restart or stop

Sometimes, the console fails to restart or stop services when running a stream service with a network service account. When the console fails, the service appears in the started state, however, the console prevents you from restarting or stopping the Stream Service.

> **Tip:**

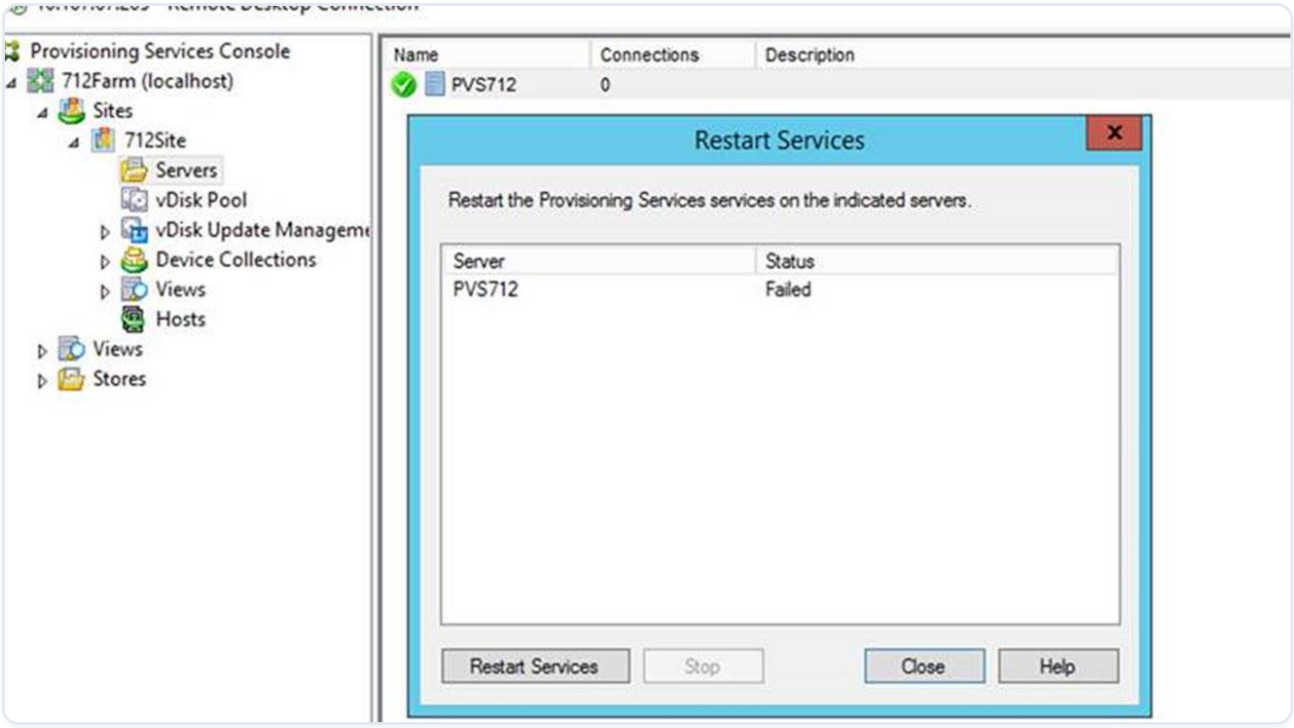
> By default, a network service account does not have permissions to start/stop services.

> For example, if services are configured with a network services account, running the configuration wizard results in an error condition. The status appears as running and streaming the virtual disk, however, the service cannot be restarted or stopped:



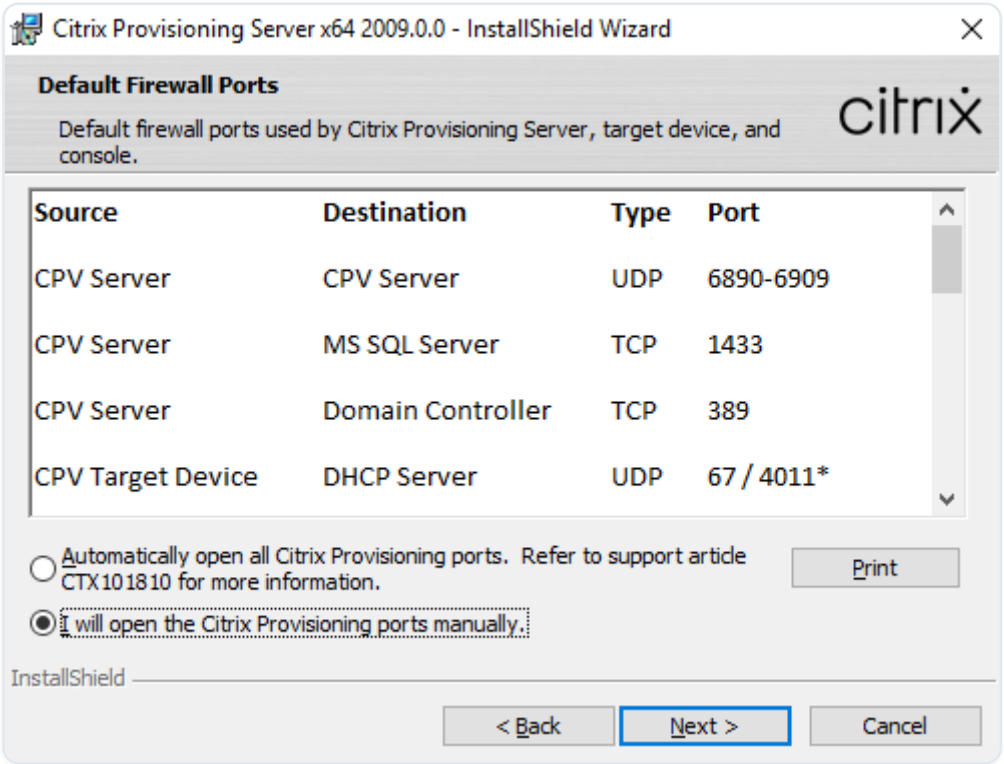
You can resolve this issue by associating the stream service with a specific account which has the required permissions to access the database. If the services are configured with a specific account, like `anuj.com\administrator`, the status appears as started. You can restart or stop the services from the provisioning console:





Open all default provisioning server's Windows firewall ports

The Citrix Provisioning server installation includes the option to open all the default server's Windows firewall ports. This configuration is useful for administrators who want to facilitate the installation process by automatically opening all Citrix Provisioning ports, without manually specifying which ports to open.



During installation, use one of the following options in the **Default Firewall Ports** installation screen:

- Automatically open all Citrix Provisioning ports
- I will open the CPV ports manually

> **Tip:**

> The **Default Firewall Ports** screen is available only if the Windows firewall is active.

Important considerations when setting up a provisioning server

When you initially set up a provisioning server, the following message might appear: *Windows Firewall is on. It will interfere with the operation of services. Either turn it off or open the necessary ports*. For more information, see Communication Ports Used by Citrix Technologies and Open Windows firewall ports.

Provisioning server performance updates

This release of Citrix Provisioning introduces updates to provisioning server performance statistics. These statistics allow other Citrix applications to determine the state of provisioned servers by introducing a performance counter provider that generates dynamic information about the provisioning server.

> **Note:**

> Citrix Provisioning version 1909 introduced functionality related to this enhancement for provisioned target devices. See What's new for more information.

How it works

This version adds a performance counter provider that captures dynamic information about the provisioning server by using an external application running on a server or a remote machine. This application queries the performance data of the server using Windows Performance Counter. The provider does not duplicate information obtained from the system using standard Windows objects, such as CPU, memory, disk, or network configuration information.

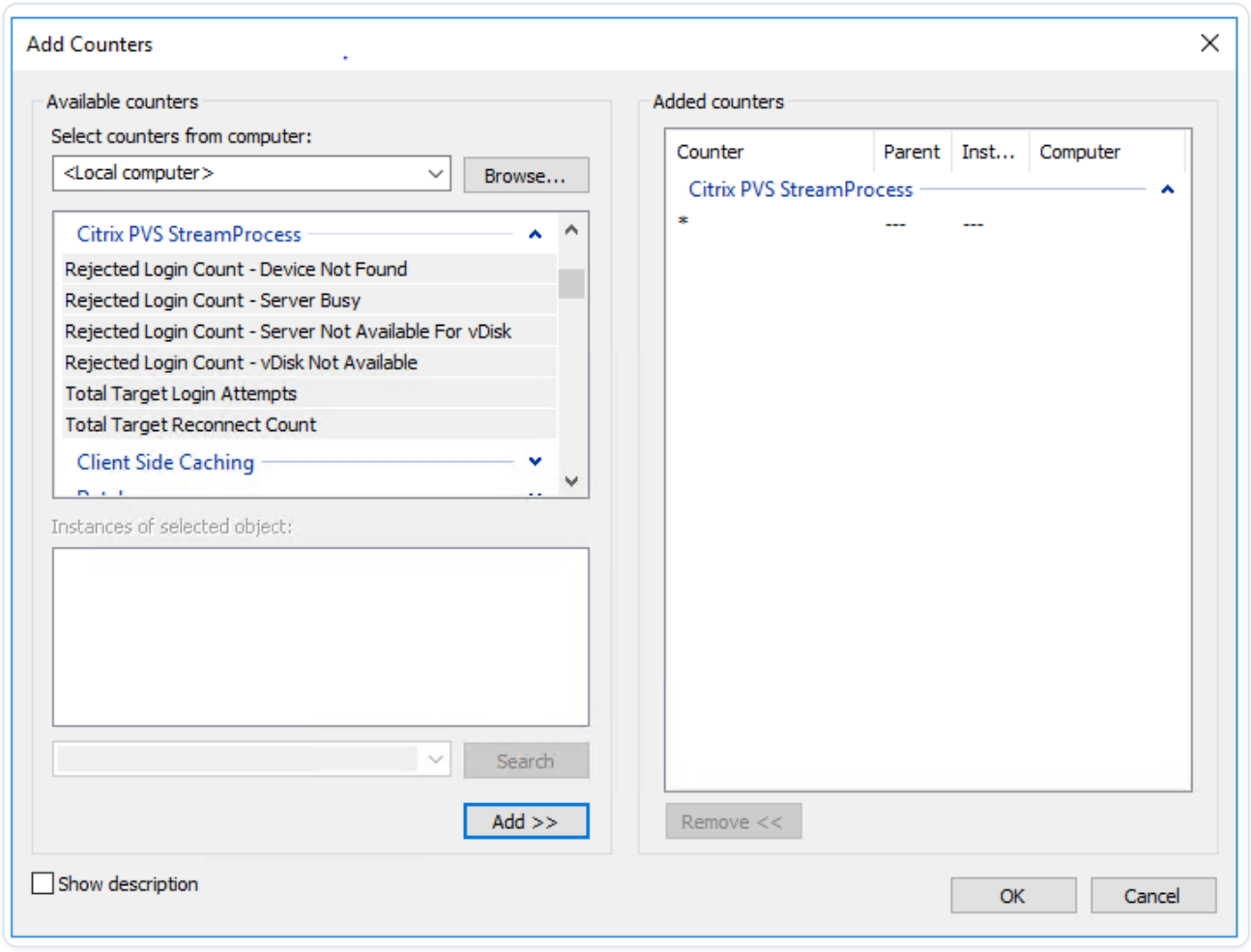
Consider:

- New Windows events containing database and stream services restart events are written to the Windows event log.

- The state of provisioned servers is obtained from the Citrix Provisioning object oriented PowerShell API.
- The Citrix Provisioning server installer registers the newly installed performance counter provider.

Updated performance counters

Installing this version adds and registers an updated performance counter on each provisioned server as part of the standard installation and upgrade process. The following image illustrates the counter as part of the StreamProcess:



The updated StreamProcess includes the following extra performance counters:

CounterSet: Citrix Provisioning StreamProcess

The provider creates the `PVS_Target` and `PVS_VDisk WMI` objects in the `root/Citrix/PVS` namespace. Each provisioned target device has a single instance of the `PVS_Target` object. The `PVS_Target` object provides information about the installed Citrix Provisioning version, and statistics for the latest boot operation.

COUNTER NAME	TYPE	DESCRIPTION
Total Target Login Attempts	perf_counter_large_rawcount	The total number of target device login attempts.
Total Target Reconnect Count	perf_counter_large_rawcount	The total number of target device reconnects.
Rejected Login Count - Device Not Found	perf_counter_large_rawcount	The number of target device logins that were rejected because the device was not found in the database.
Rejected Login Count - virtual disk Not Available	perf_counter_large_rawcount	The number of target device logins that were rejected because the virtual disk was not available for the device.
Rejected Login Count - Server Busy	perf_counter_large_rawcount	The number of target device logins that were paused because the maximum number of devices a server allows to boot was reached.
Rejected Login Count - Server Not Available For virtual disk	perf_counter_large_rawcount	The number of target device logins that were rejected because no servers were available for the virtual disk.
Vdisk WRITE failed	perf_counter_large_rawcount	Total count of failed attempts to write to a vDisk file.
Vdisk READ failed	perf_counter_large_rawcount	Total count of failed attempts to read from a vDisk file.
IO-Reply Send failed	perf_counter_large_rawcount	Total count of failed attempts to send vDisk IO replies.
Device Count Active	perf_counter_large_rawcount	Count of devices that this provisioning server is currently streaming.

COUNTER NAME	TYPE	DESCRIPTION
Device Count Timeout	perf_counter_large_rawcount	Total count of devices that have no heartbeat or IO activity for 90 seconds (default) and are timed out by the Citrix Provisioning server.
Device Count Cache Failover	perf_counter_large_rawcount	Count of devices configured to use a local disk for write cache, but unexpectedly fail over to use the write cache on the server.
Device Count Forced Reconnect	perf_counter_large_rawcount	Total count of devices that are forced by the provisioning server to reconnect.

The StreamProcess writes the following new events to the Windows Event log:

- DB online to offline with offline database support enabled
- DB online to offline with offline database support disabled
- Offline database support enabled event
- Offline database support disabled event

The StreamService writes the following new events to the Windows Event log:

- Stream process restart event
- Management daemon restart event
- Notifier restart event
- Inventory restart event

Event IDs logged by the stream process

EVENT ID	EVENT MESSAGE
200	Exception in %1!s! called from %2!s!:%3!d!.
201	DbAccess error: <%1!s!> <%2!i!> (in %3!s! called from %4!s!:%5!d!).

EVENT ID	EVENT MESSAGE
202	There was an error reading the configuration file. The default values will be used.
204	CSSInitialContact::DispatchPacket received invalid opcode %X.
205	Login failed for device %1!s! -- %2!s!.
206	Login failed for unknown device -- %s.
207	Device %1!s! moved to %2!s! for IO.
208	Secure user authorization for %s FAILED: Account Disabled.
209	Secure user authorization for %s FAILED: No matching user.
210	Switching to server side caching for device %s.
211	AcquireLock failed for vdisk id = %1!i!, device id = %2!i!, status = %3!i! <%4!s!>.
212	ReleaseLock failed for locker id = %1!i!, status = %2!i! <%3!s!>.
213	Encountered unexpected exception in DispatchDebugRequest. LogLevel=%d.
214	Database is back ONLINE. Last offline mode lasted for %1!d! days, %2!d! hours, %3!d! minutes, %4!d! seconds.
215	StreamProcess is terminating because no IP addresses is active for server %s.
216	DB is OFFLINE and Offline database support is enabled.
217	DB is OFFLINE and Offline database support is disabled.

EVENT ID	EVENT MESSAGE
218	Offline database support enabled.
219	Offline database support disabled.
220	CSSServerCache recv failed. Thread is down. WSAEnabled_ = %1!d!, WSA-LastError = %2!X!, LastError = %3!X!.
221	CSSInitialContact recv failed. Thread is down. WSAEnabled_ = %1!d!, WSA-LastError = %2!X!, LastError = %3!X!
222	CSSProtocol recv failed. Thread is down. WSAEnabled_ = %1!d!, WSA-LastError = %2!X!, LastError = %3!X!.
223	Unsupported license SKU is read from database. Use default on-premises license with trade-up enabled.
224	Cannot read server preshared key.
225	Cannot allocate read buffer in CSSProtocol thread.
226	Cannot allocate buffers in CSSProtocol thread.
227	CSSProtocol::DispatchLoginMsg received invalid opcode %X.
228	CSSProtocol::DispatchAdminMsg received invalid opcode %X.
229	CSSProtocol::DispatchDiskIOMsg received invalid opcode %X.
230	Device %1!s! boot time: %2!d! minutes %3!d! seconds.
231	Login initiated for device %1!s!, LoginType: %2!d!.

EVENT ID	EVENT MESSAGE
232	Login complete for device %s.
233	HandleSpecialClientBoot: Invalid Special Boot Code %X.
234	Detected one or more hung threads. Please send a problem report to support.
235	Device %s has powered down.
236	Service granted for device %1!s!, IP:%2!s!, Reconnect: %3!d!, ContextReuse: %4!d!.
237	Login failed (error code: %1!X!) for device %2!s!: %3!s!.
238	Login failed (error code: %1!X!) for unknown device at %2!s!: %3!s!.
239	found empty service tag -- will result in a blank device name!.
240	Device %1!s!, MAC=%2!s!, id=%3!d! cloned from template.
241	Stream Service server cache invalid opcode received %X.
242	StreamProcess is terminating because it cannot find the installation path.
243	StreamProcess is terminating because of a management interface initialization error.
244	StreamProcess is terminating because it failed to create a db access interface for locating the server record for %s.
245	StreamProcess is terminating because it cannot locate server record for %s.

EVENT ID	EVENT MESSAGE
246	StreamProcess is terminating because no IP addresses were found in database for server %s.
247	StreamProcess is terminating because no valid IP addresses are configured for server %s. Please check your server IP assignments and network cables.
248	StreamProcess is terminating because it cannot retrieve IP address information.
249	StreamProcess is terminating because of a helper module initialization error.
250	StreamProcess is terminating because it cannot open initial contact port %d.
251	StreamProcess is terminating because it failed to initialize the management interface with the following exception: %s.
252	IP address unavailable.
253	StreamProcess is terminating because it cannot open protocol object port %d.
254	StreamProcess is terminating because it cannot open secondary protocol object port %d.
255	StreamProcess is terminating because it failed to load manager library.
256	StreamProcess is terminating because it failed to link manager function.
257	StreamProcess is terminating because it failed to create a management interface.

EVENT ID	EVENT MESSAGE
258	StreamProcess is terminating because it can't get a valid dbAccess object from the management interface.
259	StreamProcess is terminating because it failed to initialize the database interface.
260	Received signal to shutdown while waiting for database.
261	Unexpected exit of idle routine WaitForSingleObject.
262	Database file not found. Please check your database path configuration. If you are using a network share please make sure your StreamService is running from an account with permission to access the network share
263	Database design mismatch. You appear to be using a database from an incompatible software version. Please upgrade your database and restart your StreamService.
264	Database file access denied. Please check your database write permissions. If you are using a network share please make sure your StreamService is running from an account with permission to access the network share.
265	Database connection string. Please check your database connection settings in the registry.
266	Database closed. This is an internal error. Please contact technical support.
267	Cannot establish a connection to the database. Server may be down or it may be a configuration error.

EVENT ID	EVENT MESSAGE
268	Cannot establish a connection to the database because the server cannot be found. Please check your database connection settings in the registry and the network path to your server.
269	Cannot establish a connection to the database because an attempt to log in failed. Please check your database connection settings in the registry and your permissions on your database server.
270	Unmapped database error. This is an internal error. Please contact technical support.
271	Undefined database error. This is an internal error. Please contact technical support.
272	Exception in %s().
273	Stream Process Started.
274	Stream Process Stopped.
275	CSSProtocolModule::TimerThread() cannot create db access.
276	StreamProcess IP %s is disconnected or non-functional.
277	StreamProcess IP %s is disconnected or non-functional, or paired IPSec address is non-functional.
278	Terminating StreamProcess.
279	Exception in thread %1!s! near %2!s!:%3!d!.
280	StreamProcess cannot find server record for %s in ServerConfigChangedNotification.
281	Exception generated by streamprocess.exe. Please send streamprocess.dmp to support.

EVENT ID	EVENT MESSAGE
282	Cannot update the VHD timestamp.

Device collections

Device collection properties are on the following tabs:

- General
- Security
- Auto-Add

General tab

FIELD	DESCRIPTION
Name	The name of this device collection.
Description	Describes this device collection.
Template target device	To use the settings of an existing target device as the template, select that device from the menu, then click **OK**.

Security tab

FIELD	DESCRIPTION

Auto-Add tab

FIELD	DESCRIPTION
Template target device	Displays the name of the target device. Or, if a device was previously selected, or `\<No template device>` if a device was not selected. Use the menu to select a device to use as the template for adding new devices to this collection. To view a selected device's

FIELD	DESCRIPTION
	properties, click **Properties** (read-only dialog appears).
Prefix	Enter a static prefix that helps identify all devices that are being added to this collection. For example: 'Boston' to indicate devices located in Boston. The prefix can be used with the suffix, but is not required if a suffix is provided. The entire device name can have a maximum of 15 characters (the prefix length + number length + suffix length). For example, the following device names are considered valid: **Boston**000**Floor2** (prefix, incrementing number length, and suffix provided. The maximum of 15 characters has been reached), **Boston**000 (no suffix is provided), 000**Floor2** (no prefix is provided). The prefix cannot end with a digit. The prefix and suffix combination must be unique in each collection.
Number length	Enter the length of the incrementing number to associate with the devices being added to this collection. This number is incremented as each device is added. For example, if the number length is set to 3, Citrix Provisioning starts naming at 001. It stops naming or adding devices after the number reaches 999.Enable the Zero fill option to automatically add the necessary number of preceding zeros to a numbers length. For example, if the numbers length is equal to 3, then the first target device number would be assigned as '001'. Enable the Zero fill option to automatically add the necessary number of preceding zeros to a numbers length. For example, if the numbers length is set to '4', then the first target device number would be assigned as '0001'. The number length must have a minimum of three digits and a maximum of 9 digits.

FIELD	DESCRIPTION
Suffix	Enter a static suffix that helps to identify all devices being added to this collection. For example: Boston001**Floor2** might be helpful to indicate the floor where these devices reside. The suffix can be used with the prefix, but is not required if a prefix is provided. The entire device name can have a maximum of 15 characters (the prefix length + number length + suffix length). The suffix cannot start with a digit. The prefix and suffix combination must be unique in each collection.
Last incremental number	Indicates the last incremental number that was assigned to a device name in this collection. This number can be reset to '0' but cannot be lower than the highest number for the same Prefix/Suffix combination.

Creating a device collection

To create a device collection:

1. In the Citrix Provisioning™ console, right-click on the **Device Collections** folder where the new collection exists, then select the **Create device collection** menu option. The **Device Collection Properties** dialog appears.
2. On the **General** tab, type a name for this new device collection in the **Name** text box. Include a description of this collection in the **Description** text box, then click the **Security** tab.
3. Under the **Device Administrators** list, click **Add**. The **Add Security Group** dialog appears.
4. To assign a group with the Device Administrator role, type or select the appropriate domain and group name in the text box, then click **OK**.
5. Optionally, repeat steps 2 and 3 to continue assigning groups as device administrators.
6. Under the **Device Operators** list, click **Add**. The **Add Security Group** dialog appears.
7. To assign a group with the Device Operator role, type or select the appropriate domain and group name in the text box, then click **OK**.
8. Optionally, repeat steps 2 and 3 to continue assigning groups as device operators.
9. Click **OK** to close the dialog box.

Deleting a device collection

Deleting a device collection removes any target device member records within the collection. Recreate the records by manually adding them or using the Auto-add feature.

> **Tip**
>
> Deleting a target device also deletes that device from any views that it was associated with.

> If target devices are members of collections within the same site, the members of one collection can be moved to other collections. Once a collection is moved to another one, the original collection can be deleted. When you need to move a device collection to a different site or that site becomes obsolete, use the export and import features to add the devices to a collection in another site. The original collection can then be deleted.

To delete a device collection:

1. In the Citrix Provisioning console tree, right-click on the collection folder that you want to delete, then select the **Delete** menu option. A confirmation message appears.
2. Click **OK** to delete this collection. The collection no longer displays in the console tree.

Target devices

After you install and configure provisioning components, a vDisk is created from a device's hard drive. This disk is created from a snapshot of the OS and application image, it then stores that image as a vDisk file on the network. The device that is used during this process is seen as a main target device. The devices that use those vDisks are called target devices.

Configuring target devices that use vDisks

Citrix Virtual Apps and Desktops™ with vDisk technology is a high-performance enterprise desktop virtualization solution that makes VDI accessible to workers requiring personalized desktops using pooled, static virtual machines.

The wizard also creates virtual machines to associate with each device. A type of catalog in Citrix Studio allows you to preserve the assignment of users to desktops (static assignment). The same users are assigned the same desktop for later sessions.

Target device operation and performance statistics

Use Citrix Provisioning™ to view target device operations and performance statistics, including:

- a WMI provider for static information about the target device.
- a performance counter provider for dynamic information about the target device.
- an external application running on the target device or the remote machine. This application queries objects using a WMI API to determine if they are running on a provisioned target and to gather information related to the configuration and state of the device.

As part of the standard Citrix Provisioning target device installation, a WMI provider DLL is installed and registered on each provisioned target device. This DLL obtains target device information from the BNIStack driver.

How it works

The provider creates the `PVS_Target` and `PVS_VDisk WMI` objects in the `root/Citrix/PVS` namespace. Each provisioned target device has a single instance of the `PVS_Target` object. The `PVS_Target object` provides information about the installed Citrix Provisioning version, and statistics for the latest boot operation.

If no instance of `PVS_Target` exists when the WMI provider queries the target device, then the device is not a Citrix Provision target device.

The PVS_Target object

The following table provides information about the `PVS_Target` object:

ITEM NAME	TYPE	UNIT	DESCRIPTION
Target_Software_Version	String	-	PVS target version
Boot_Time_In_Sec	Int	seconds	The number of seconds elapsed during the boot phases of the operating system
Boot_Retry_Count	Int	-	Retry count during boot

ITEM NAME	TYPE	UNIT	DESCRIPTION
Boot_Bytes_Read_MB	Int	MB	Number of bytes read during boot
Boot_Retry_Written_MB	Int	MB	Number of bytes written during boot

The PVS_VDisk object

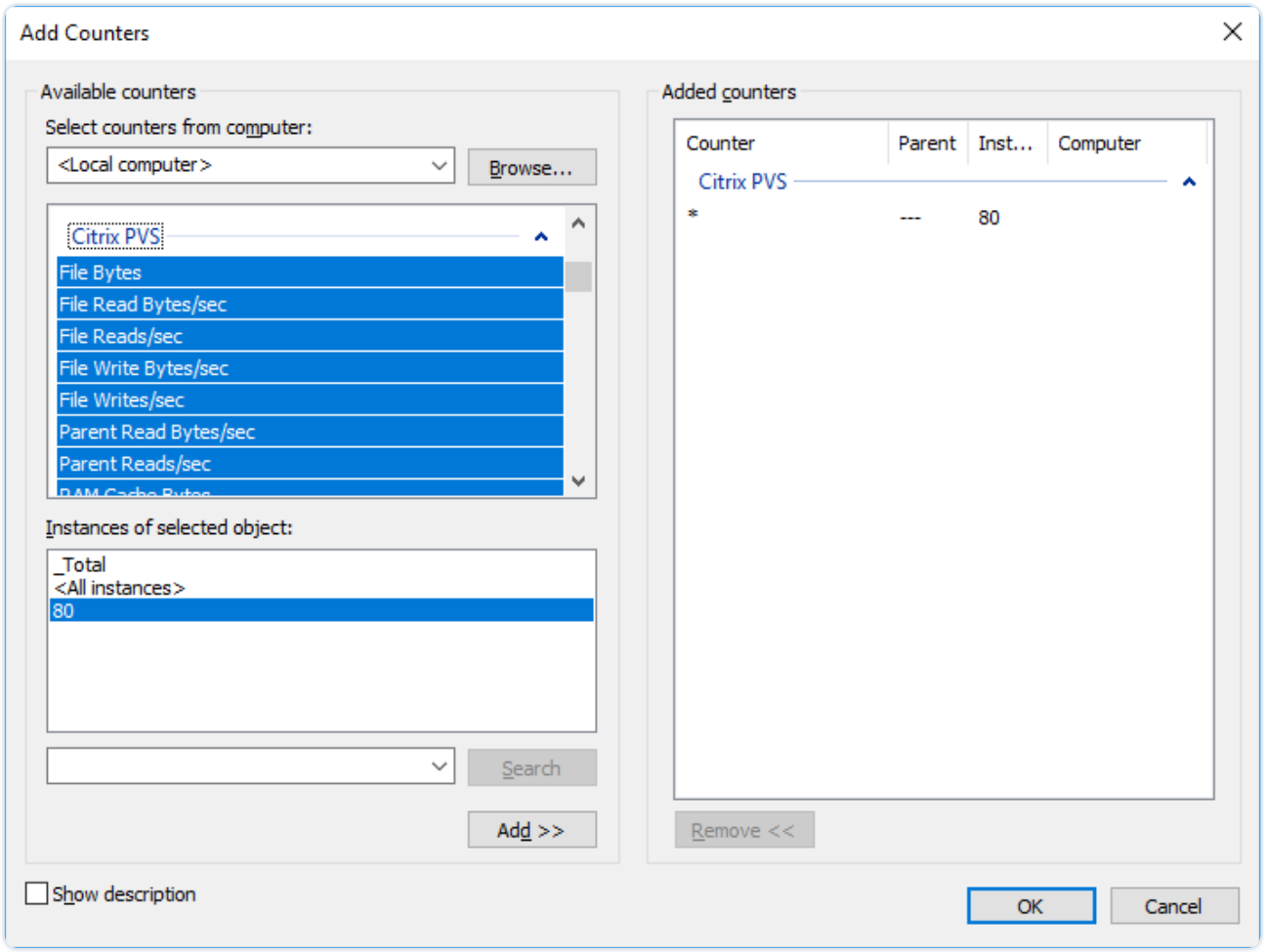
One instance of the `PVS_VDisk` object exists on the provisioned target device. This object contains information about the vDisk, the write cache mode and cache disk size.

The table below provides information about the `PVS_VDisk` object:

ITEM NAME	TYPE	UNIT	DESCRIPTION
VDisk_Name	String	-	vDisk file name
Write_Cache_Type	String	-	Write cache type being used
Write_Cache_Volume_Size	Int	MB	Configured write cache volume size
Boot_From	String	-	Boot from vDisk or local hard disk
Write_Cache_Volume_Drive_Letter	String	-	Write cache volume drive letter

Updated performance counters

Citrix Provisioning includes a performance counter that is automatically installed and registered on each provisioned target device.



The BNIStack driver provides the following performance counters:

COUNTER NAME	TYPE	DESCRIPTION
UDP retry	perf_counter_counter	PVS UDP retry count
Server reconnect	perf_counter_counter	PVS server reconnect count

Consider the following:

- The provisioned target device installer registers the WMI and performance counter providers. No additional installation options require configuration on the provisioned target device.
- The current `CVhdMp` performance counter provider only supports VHDX for target devices using **Cache in device RAM with overflow on hard drive**.

Performance counters provided by the CVhdMp driver

- use the Citrix Provisioning Imaging Wizard. In the **Microsoft Volume Licensing** screen, click the appropriate license management option for the vDisk. Click the **Key Management Service**

(KMS) radio button, then click the **Accelerated Office Activation** check box. Select **Next** to apply the configuration change to the vDisk and continue configuring it.

COUNTER NAME	TYPE	DESCRIPTION
File bytes	perf_counter_large_rawcount	The VHDX file size
File reads/sec	perf_counter_counter	The rate of reads from VHDX file in operations per second
File writes/sec	perf_counter_counter	The rate of writes to VHDX file in operations per second
File read bytes/sec	perf_counter_bulk_count	The rate of reads from VHDX file in bytes per second
File write bytes/sec	perf_counter_bulk_count	The rate of writes from VHDX file in bytes per second
RAM cache types	perf_counter_large_rawcount	The amount of memory used by RAM cache
RAM reads/sec	perf_counter_counter	The rate of reads from RAM cache in operations per second
RAM writes/sec	perf_counter_counter	The rate of writes to RAM cache in operations per second
RAM read bytes/sec	perf_counter_bulk_count	The rate of reads from RAM cache in bytes per second
RAM write bytes/sec	perf_counter_bulk_count	The rate of writes to RAM cache in bytes per second
Parent reads/sec	perf_counter_counter	The rate of reads from parent in operations per second
Parent read bytes/sec	perf_counter_bulk_count	The rate of reads from parent in bytes per second

Adding target devices to the database

To create target device entries in the **Citrix Provisioning database**, select one of the following methods:

- Using the console to Manually Create Target Device Entries
- Using Auto-add to Create Target Device Entries
- Importing Target Device Entries

After the target device exists in the database, you can assign a vDisk to the device. See assign a vDisk to the device for more details.

Using the console to manually create target device entries

1. In the console, right-click on the **Device Collection** where this target device is to become a member, then select the **Create Device** menu option. The **Create Device** dialog appears.
2. Type a name, description, and the MAC address for this target device in the appropriate text boxes.

   > **Note:**
   >
   > If the target device is a domain member, use the same name as in the Windows domain. When the target device boots from the vDisk, the machine name of the device becomes the name entered. For more information about target devices and Active Directory or NT 4.0 domains, see *Enabling Automatic Password Management*.

3. Optionally, if a collection template exists for this collection, enable the check box next to **Apply the collection template to this new device**.
4. Click the **Add device** button. The target device inherits all the template properties except for the target device name and MAC address.
5. Click **OK** to close the dialog box. The target device is created and assigned to a vDisk.

> **Note:**
>
> If the MAC address from the target device does not match with the hypervisor MAC address, then the vDisk fails to boot with an error message **No entry found in database for device when booting from vDisk**.

Importing target device entries

Target device entries can be imported into any device collection from a .csv file. The imported target devices can then inherit the properties of the template target device that is associated with that collection. For more details, see Importing Target Devices into Collections.

Using the auto-add wizard

The auto-add wizard automates the configuration of rules that automatically add new target devices to the Citrix Provisioning database using the auto-add feature.

The Auto-Add Wizard can be started at the Farm, Site, Collection, or Device level. When started at a level lower than farm, the wizard uses that choice as the default choice. For example, if it is started on a particular target device, it will:

- Select the **Site** for that device as the **Default Site** choice in the combo-box.
- Select the **Collection** for that device as the **Default Collection** choice in the combo-box.
- Select that device as the **Template Device** choice in the combo-box.

The wizard displays each page with choices pre-selected based on the location from which the auto-add wizard was started.

A provisioning farm administrator turns auto-add *on* or *off* and selects the default site.

A site administrator selects the default site if it is a site in which that administrator controls. If the site administrator is not the administrator of the currently selected default Site, then that administrator can only configure sites to which they have access.

To configure Auto-Add settings (the default collection of a site, template device for the default collection and target device naming rules):

1. On the console, right-click on the farm, then select the **Auto-Add wizard**. The **Welcome to the Auto-Add Wizard** page appears.
2. Click **Next**. The **Enable Auto-Add** dialog appears.

> **Note:**
>
> Only a farm administrator can change settings on this page.

3. Check the box next to **Enable Auto-Add** to enable this feature, then click **Next**. The **Select Site** page appears.

> **Note:**
>
> Site administrators can only select sites to which they have permissions.

4. From the **Site** menu, select the site where devices are added, then select **Next**. The **Select Collection** page displays with the default collection selected.
5. Accept the default collection or select a different collection from the **Collection** menu, then click **Next**. The **Select Template Devices** page appears.
6. Select the device to use as a template, so that new devices inherit the existing target device's basic property settings, then click **Next**.
7. To view the selected device's properties, click **Properties**. A read-only dialog displays the selected device's properties. Close the dialog after reviewing the properties.
8. Click **Next**. The **Device Name** page displays.
9. Enter a static prefix that helps identify all devices that are being added to this collection. For example: 'Boston' to indicate devices located in Boston.

> **Note:**
>
> The prefix can be used with the suffix, but is not required if a suffix is provided. The entire device name can have a maximum of 15 characters (the prefix length + number length + suffix length). For example, the following device names are considered valid:

- **Boston**000**Floor2** (prefix, incrementing number length, and suffix provided. The maximum of 15 characters has been reached)
- **Boston**000 (no suffix is provided)
- 000**Floor2** (no prefix is provided)

The prefix cannot end with a digit.

10. Enter the length of the incrementing number to associate with the devices being added to this collection. This number is incremented as each device is added. For example, if the number

length is set to 3, naming starts at 001 and stops naming or adding devices after the number reaches 999.

Note:

Enable the Zero fill option to automatically add the necessary number of preceding zeros to a numbers length. For example, if the numbers length is set to '4', then the first target device number would be assigned as '0001'.

The number length must have a minimum of three digits and a maximum of 9 digits.

Enter a static suffix that helps to identify all devices being added to this collection. For example: Boston001**Floor2** might be helpful to indicate the floor where these devices reside.

The suffix can be used with the prefix, but is not required if a prefix is provided.

The entire device name can have a maximum of 15 characters (the prefix length + number length + suffix length).

The suffix cannot start with a digit.

The prefix and suffix combination must be unique in each collection.

1. Click **Next**. The **Finish** dialog appears.
2. Review all Auto-Add wizard settings, then click **Finish**. Auto-Add is now configured.

Disabling a target device

The Disable Target Device feature prevents a new target device from booting. Each time a new target device boots with the auto-add option enabled, a new record is automatically created in the database. The following message appears on the target device:

```
This target device has been disabled. Please Contact your system administrator.
```

Once contacted, the system administrator can validate the target device. After the administrator disables the option, the target device can boot successfully.

To disable or enable a target device, in the console, right-click on the target device. Select the **Disable or Enable** menu option.

Tip:

To disable all target devices added to a collection, enable the **Disable target device** option on the template target device.

Deleting a target device

To delete a target device:

1. In the Console, right-click on the target devices you want to delete within the collection.Multiple selections can be made in the Details view. Select the **Delete** menu option.
2. Click **Yes** to confirm the delete request. The target device is deleted from the collection and any associated views. However, the vDisk image file for the target device still exists.

Improving performance with asynchronous I/O streaming

In Citrix Provisioning releases before version 1808, a target device served incoming operating system storage requests by traversing through three different layers: RAM cache, VHDX file, and network streaming. This process occurred sequentially to complete a request. This traversing led to less than optimal performance due to the latency introduced when waiting for sub-I/O completion, before submitting a new sub-I/O request.

Target devices support asynchronous I/O in all three layers of provisioning write cache components: RAM cache, the VHDX file, and network streaming, effectively improving performance.

Important:

Asynchronous I/O streaming provides better performance, but comes with higher, temporary memory consumption. Citrix recommends that you test this feature in a non-production environment to verify that the performance is favorable before deploying to production.

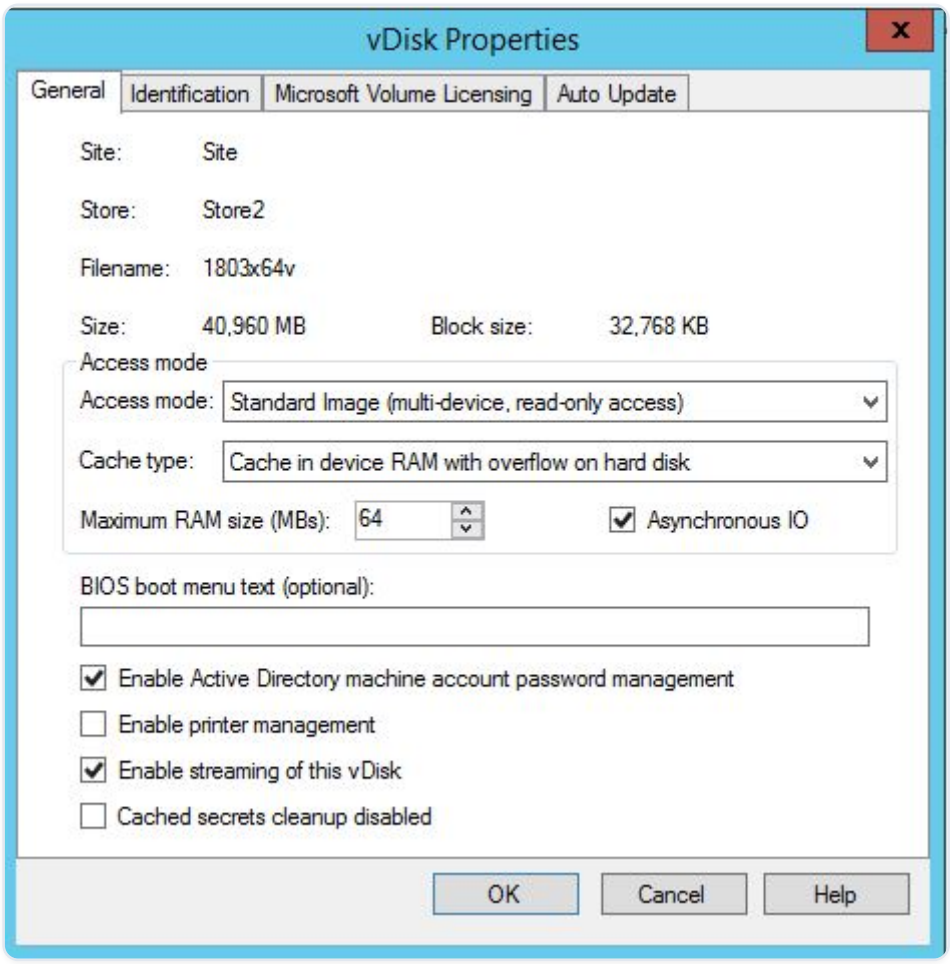
The following vDisk cache modes support asynchronous I/O:

- Cache in device RAM with overflow on hard drive
- Cache on server persistent

> **Note:**
>
> The **Cache on hard disk** feature option currently appears in the product but does not function.

Enable asynchronous I/O using the provisioning console

This release improves asynchronous I/O streaming functionality by allowing you to enable it for a vDisk directly from the Provisioning Console. In the vDisk properties screen, select **Asynchronous IO**.



Using the Boot Device Management utility

The Boot Device Management utility is an optional method for providing IP and boot information (boot device) to target devices. It is an alternative to using the traditional DHCP, PXE, and TFTP methods. When the target device starts, it obtains the boot information directly from the boot device. With this information, the target device is able to locate, communicate, and boot from the

appropriate Citrix Provisioning™ server. After user authentication, the server provides the target device with its vDisk image.

The following boot devices are supported:

- USB
- CD-ROM (ISO)
- Hard Disk Partition

Wireless NICs are not supported.

> **Warning:**
>
> When selecting an entire hard drive as a boot device, all existing disk partitions are erased and re-created with a single active partition. The targeted partition is reserved as a boot device, and is not used by the operating system or by data.

> When a hard disk partition is selected as boot device, the selected disk partition data is deleted and set as an active partition. This active partition becomes the boot device.

Configuring boot devices

Boot devices are configured using the Boot Device Management utility. This wizard-like application enables you to quickly program boot devices.

After installing the boot device, complete the procedures that follow. Consider the following:

- The target device settings in the Citrix Provisioning console are set to boot from the vDisk. The actual device is set to boot from the hard disk first.

1. From the Citrix Provisioning product installation directory, run **BDM.exe**. The **Boot Device Management** window opens and the **Specify the Login Server** page appears.
2. If using IPv6 networking, select **Use IPv6 address** checkbox. This changes the format used or displayed on the server IP address box.
3. Under **Server Lookup**, select the radio button that describes the method to use to retrieve Provisioning Server boot information:

- Use DNS to find the Provisioning Server from which to boot. If this option is selected and the **Use DHCP to retrieve Device IP** option is selected your DHCP server must be configured to provide the DNS Server.

  Note: The boot device uses Host name plus DHCP option 15 (Domain Name, which is optional) as the FQDN to contact the DNS server to resolve the IP address.

  If you are using high availability, specify up to 32 Provisioning Servers for the same host name on your DNS server.

- Use the static IP address of the Provisioning Server from which to boot. If you select this option, click **Add** to enter the following Provisioning Server information:

  - IP Address
  - Port (default is 6910)

  In high availability implementations, enter up to 32 Citrix Provisioning servers. If you are not using high availability, enter only one. Use the **Move Up and Move Down** buttons to sort the Provisioning Servers boot order. The target device selects a random entry from the list to log in to at boot time. If this fails, the target device selects the next entry and then follows the list in order from that entry.

4. In the **Burn the Boot Device** dialog, configure the target device IP. If the **Use DNS to find the Server** option is selected and your DHCP service does not provide option 6 (DNS Server), enter the following required information:

   - Primary DNS Server Address
   - Secondary DNS Server Address
   - Domain Name

5. Configure the **Boot Device** properties. Options are:

   - Citrix ISO Image Recorder: the tool generates an ISO file that can be attached to the CD drive of the target. In this case, configure the target device to boot from the CD drive.
   - Citrix VHD Image: the tool creates a VHD boot disk image that can be attached to the target device as the disk to boot from. In this case, configure the target VM to boot from hard disk.
   - Existing boot disk: this option allows you to update the current hard disk that the device boots from to add a new boot option. In this case, no change to the boot order is required

and on next boot the VM boots form the network using the configured parameters. The name here reflects the Windows device name of the boot disk.

6. If the device has multiple network adapters, you can choose which one to boot from when streaming. The default is the first NIC.
7. Click **Burn**. A message appears to acknowledge that the boot device was successfully created.
8. Click **Exit** to close the utility.
9. If the boot order must be changed, boot the target device and enter the **UEFI Setup**. Under the **Boot Sequence**, move the boot device to the top of the list of bootable devices. Save the change and boot the target device.

After the boot device is programmed, configure a target device boot sequence using the console's **Target Device Properties** dialog. These boot behaviors are used after a target device connects to a provisioning server.

Streaming Linux target devices

This article provides information about streaming Linux target devices. Using the Linux streaming feature with Citrix Provisioning, you can provision Linux virtual desktops in the Citrix Virtual Apps and Desktops environment. For more information about the Linux streaming feature, see Create Linux VDAs using Citrix Provisioning.

Citrix Provisioning™ version 2203 LTSR supports both BIOS and UEFI boot modes for Linux targets. Versions 2311 and 2402 LTSR support only BIOS boot mode. However, for version 2407 and later, no boot mode is supported for Linux targets.

> **Important:**

> We recommend that you use the most recent installation package of Citrix Provisioning. Use the package based on your Linux distribution. Citrix Provisioning Server 2109 or later is required to use Linux streaming agent 2109 and later.

> Consider the following when provisioning Linux target devices:

- When you use Citrix Provisioning to stream Linux target devices, create a separate boot partition on the single shared-disk image so that the provisioned devices can boot as expected.

- Sometimes, the client drive cannot be mapped to a provisioned Linux VM session. To resolve this issue, halt the CDM service using `service ctxcdm stop`, before installing the Citrix Provisioning target device, then run the `pvs-imager` command to convert it.
- Linux streaming only supports Winbind as the tool for joining a Windows domain. Winbind provided by Samba 4.5 and newer is supported, including older releases.
- When you enable RAM cache for the Linux device, set the cache size to 8 MB (the minimum value). Linux uses as much RAM as necessary, including all available memory, for the write cache. The amount specified in the console is the amount reserved up front. Citrix® recommends that you reserve as little as possible, which effectively allows Linux to manage memory usage.
- The target device name in the Citrix Provisioning imager UI typically defaults to `im\_localhost`. This value must be changed when you create more than one vDisk. Using the same target device name causes the imager command to fail.
- Installation (and subsequent updates) must be done in super user mode. There are two ways to install as a super user:
  - Enter user mode in a terminal using the `su` command.
  - Enter `sudo` before the command. For example, `sudo yum install tdb-tools`; enter `sudo` for every command.
- The Linux client's system clock must be synchronized by using the active directory controller.
- VMM is not supported.
- The write cache drive must have the label `PVS_Cache` for it to be used as a write cache. The entire partition is used.
- English localizations are displayed on non-English installations.
- SE Linux is not supported.
- Targets running on XenServer (formerly Citrix Hypervisor™) must run in HVM mode.
- After booting a Linux target device, a warning message might display indicating a SE Linux Alert Browser.
- The following Linux distributions are supported:
  - Ubuntu 22.04
  - Ubuntu 20.04
  - RHEL 9.2
  - RHEL 9.0

  - RHEL 8.8
  - RHEL 8.6
  - RHEL 7.9
  - Rocky Linux 9.2
  - Rocky Linux 9.0
  - Rocky Linux 8.8
  - Rocky Linux 8.6
  - SUSE 15.5

- Streamed Ubuntu 20.04 VMs hosted on ESXi get the IP address through DHCP. To resolve this issue, configure the VM to use the MAC address as a unique ID to retrieve an IP address through DHCP.
- Create a vDisk using UEFI boot from a master VM using UEFI boot.

Installation

To install the Linux Streaming component, you must be logged in while an administrator. If installing, consider that the following commands must be issued in a root shell, or by using sudo privileges.

> **Note:**
>
> You can download the packages from Downloads. After you download, you can see the Linux streaming packages in `/Device/linux directory of Provisioning.iso`.

Install the Linux streaming package

For Ubuntu 22.04 distributions:

```
sudo dpkg -i pvs_<version>_ubuntu22.04_amd64.deb

sudo apt-get -yf install
```

For Ubuntu 20.04 distributions:

```
sudo dpkg -i pvs_<version>_ubuntu20.04_amd64.deb

sudo apt-get -yf install
```

For RHEL 9.2, RHEL 9.0, Rocky Linux 9.2, and Rocky Linux 9.0 distributions:

```
yum --nogpgcheck localinstall pvs_<version>_rhel9.0_x86_64.rpm
```

For RHEL 8.8, RHEL 8.6, Rocky Linux 8.8, and Rocky Linux 8.6 distributions:

```
yum --nogpgcheck localinstall pvs_<version>_rhel8.6_x86_64.rpm
```

For RHEL 7.9 distributions:

```
yum --nogpgcheck localinstall pvs_<version>_rhel7.9_x86_64.rpm
```

For SUSE 15.5 distributions:

```
zypper install pvs_<version>_suse15.2_x86_64.rpm
```

Using the GUI to create a Linux golden image

To invoke the GUI to install this feature:

1. Log in while an administrator.
2. Run the following:

   `pvs-imager`

Tip:

When the `pvs-imager` command fails due to a host name issue, verify that your network configuration is correct. Do not set the system's host name to `localhost`. On RHEL 8.4, log in with the X11 display server instead of Wayland to use the GUI. `PyQt5`, `python3-pyqt5`, or `python3-pyqtgraph` is required to use the GUI.

After running the command, the UI page displays:



Using the command line interface to install the Linux streaming feature

To invoke the command line to install this feature:

1. Log in while an administrator.
2. Run the following command:

   ```
   pvs-imager -C
   ```

The command-line installation includes two options:

- `\-C` allows you to create a vDisk
- `\-U` allows you to update an existing vDisk

The following information illustrates non-GUI related installation options for the Linux Streaming feature:

```
Usage: ./pvs-imager [-hCU] [-a|--address=&lt;IPaddr>] [-u|--
username=&lt;username>] [-p|--password=&lt;password>] [-P|--
port=&lt;port>] [-d|--domain=&lt;domain] [-S|--store=&lt;store>] [-v|--
vdisk=&lt;vdisk name>] [-s|--size=&lt;vdisk size] [-D|--
device=&lt;sourceDevice>] [-c|--collection=&lt;collection>] [-n|--
name=&lt;name>]

 Non-GUI Modes:

  -C      -  Create a new vDisk

    ---OR----

  -U      -  Update an existing vDisk



 General Options:

  -a &lt;server IP> -  Address or hostname of PVS server

  -u &lt;username>  -  Username for API login

  -p &lt;password>  -  Password for API login

  -d &lt;domain>   -  AD domain for API login

  -P &lt;port>    -  Base port for API login (default: 54321)

  -S &lt;store>   -  Store containing vDisk

  -c &lt;collection> -  Collection to store imaging device in

  -n &lt;name>    -  Device name for imaging device

  -v &lt;name>    -  vDisk name

  -s &lt;size>    -  vDisk size (Create Mode only, default: sourceDevice
size)

  -D &lt;sourceDev> -  devnode to clone

  -V      -  increment debug verbosity (up to 5 times)
```

```
-g &lt;grubMode>  -  Supported Grub settings ('debug')
```

Supported file systems for imaging are `ext4`, `xfs`, or `btrfs`.

Tip:

Debugging logs for `pvs-imager`, created using `-VVVVV` switch, are created in the folder that executed the `pvs-imager` tool. The name of the log file is `pvs-imager.log`.

About disk caching

For hard disk caching or hard disk overflow caching without the Citrix Virtual Apps and Desktops™ Setup Wizard, format the target device disk using a formatted partition. Include the label `PVS_Cache`. This object can be created with the `mkfs –L PVS_Cache` command on the target device. Any case-sensitive file system can be used for the cache, but XFS is recommended.

Tip:

An administrator can create any cache disk selection logic for their environment by writing a bash script that runs at launch time. The script would look for a cache device candidate by whatever mechanism is best suited to the environment, running `mkfs` on it, and rebooting.

When configuring disk caching:

- Citrix recommends using the Citrix Virtual Apps™ and Desktops Setup Wizard to create the Linux target device.
- Manually creating the label requires adherence to case sensitivity to avoid configuration conflicts.
- Alternately, consider using the manual method for creating the write cache.

Manually creating the write cache for a target device

By default, the Citrix Virtual Apps and Desktops Setup Wizard ignores drives that are attached to the current template. The wizard creates a write cache based on parameters you provide. Sometimes, the write cache drive encounters problems during automatic creation using the wizard, or, when the target device continuously falls back to server side cache as a result of a problem with

the created drive. To resolve these issues, manually create the object using the `mkfs –L PVS_Cache` command on the target device.

The Citrix Virtual Apps and Desktops Setup Wizard recognizes manually created write cache changes for the target device by default when you use the `UseTemplatecache` parameter. On the provisioning server running the Citrix Virtual Apps and Desktops Setup Wizard, or where the remote provisioning console points, change the registry setting:

1. Create the following registry key on the provisioning console machine to disable the template cache:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices`

`Name: UseTemplateCache`

`Type: DWORD`

`Value: 0`

1. Run the Citrix Virtual Apps and Desktops Setup Wizard. On the **Virtual machines** page change the local write cache disk size to 0 GB (default is 6 GB).

LIMITATION

The registry key `UseTemplatecache` created on the Provisioning Server running the Citrix Virtual Apps and Desktops Setup Wizard supports only PXE or ISO mode and not HDD BDM boot.

About SAN policies

Citrix Provisioning™ clients always failover to server side cache during boot when the vDisk mode is set to **Cache in device RAM with overflow on hard disk**.

> **Tip:**
>
> An option has been removed from the **Cache type** field in the **vDisk Properties** window. The option **Cache on device hard disk** is no longer available from the list because it does not support ASLR. The replacement for this field is **Cache in device RAM with overflow on hard disk**. For more information, see Features removed from future releases.

Resolving failover to server side caching during boot

1. In a provisioning target device booting in private vDisk mode or maintenance vDisk version, open a command prompt with administrator privileges.
2. Run the DiskPart utility, using the following command:

   ```
   diskpart
   ```

3. To verify the SAN policy, run the command:

   ```
   Diskpart > san
   ```

   The SAN policy is configured as **Online All for PVS target devices**. Ths configuration allows it to function correctly while in **Cache in Device RAM with Overflow on Hard Disk** mode.

4. To change the SAN policy, run the command:

   ```
   Diskpart > san policy=OnlineAll
   ```

5. Shut down the target device and change the vDisk mode to **standard image** or promote the maintenance version to **test** or **production version**.

> **Note:**
>
> The SAN policy causes the write cache drive to remain offline. During boot, the target device determines that the write cache drive is ineligible for use as a write cache. As a result, it fails over to server side cache.

Important considerations

When creating a machine template, ensure that it has a similar hard disk drive structure. The machine template must boot from a vDisk in private image mode. For example:

- To PXE boot a VM with write cache, create a VM with 1 hard disk drive.
- To use Boot Device Manager (BDM) to boot a VM with write cache, create a VM with 2 hard disk drives.

Using the Status Tray on a target device

The Virtual Disk status tray provides device and product edition information on the target device. The purpose of this tool is to aid in the management and troubleshooting of virtual disks.

> **Note:**
>
> This tool is installed automatically during the installation process.

Starting the Virtual Disk status tray

To manually start the Virtual Disk Status tray, double-click on the **Status Tray** icon in the System Tray. The **Virtual Disk Status Tray** dialog box appears.

Using the General tab

The following list describes each field on the **General** tab.

- **vDisk Information:**

  Status: Indicates the current state of the virtual disk. Values include:

  Active (target device is accessing this virtual disk) Inactive (target device is not accessing this virtual disk)

  Server: Indicates the IP address and port of the Provisioning Server providing access to the virtual disk.

  Boot from: Indicates if this virtual disk is set to boot from a local hard drive or from a virtual disk.

  Virtual Disk: Represents the name of the virtual disk accessed by the target device.

  Mode: The current access mode for the virtual disk. Values include:

  - Read only
  - Read and write

- **Version:**

  Edition identifies the edition and provides version and server-pack information.

  Build identifies the specific product build and compile date.

- **Preferences:**

  Prompt status message in system tray: Enable this option if you want the virtual disk Status Tray to automatically start when the user logs into the target device.

Show icon in system tray: To indicate connection status to the virtual disk, enable this option and the icon appears in your Windows system tray when this program runs.

Using the Statistics tab

The following list describes each field on the **Statistics** tab.

- **Boot Statistics:**

  Boot time: The number of seconds elapsed during the boot phases of the operating system. This value does not include the POST, BIOS, PXE, DHCP, or TFTP.

  Retries: The number of packet retries that occurred during the boot phases.

  Bytes Read: The total number of bytes read during the boot phases.

  Bytes Written: The total number of bytes written during the boot phases.

  Throughput: A value calculating the overall throughput of the software during the boot phases. Throughput = (Bytes Read + Bytes Written)/Boot Time (in seconds).

- **Session Statistics:**

  Uptime: The length of time the target device has been booted (HHHH:MM:SS)

  Retries: The total number of retries.

  Bytes Read: The total number of bytes read.

  Bytes Written: The total number of bytes written.

- **Diagnostic Statistics:**

  Uptime: The length of time the target device has been booted (HHHH:MM:SS)

  Retries: The total number of retries.

  Bytes Read: The total number of bytes read.

  Bytes Written: The total number of bytes written.

Setting Virtual Disk status tray preferences

On the **General tab** of the **Virtual Disk Status** dialog, the tray can be configured to run automatically when the target device starts, or started manually. Choose to have the **Virtual Disk Status tray** icon appear in your system tray.

To configure the Virtual Disk Status Tray, choose from the following methods:

- Configure the tray to appear automatically as each target device starts.
- Add the **Virtual Disk Status tray** icon to your system tray.

Configuring the tray to appear automatically as each target device starts

1. Start the Virtual Disk Status Tray, and then select the **General** tab.
2. Select **Automatically start this program** under **Preferences**. The tray starts automatically the next time the target device boots.

Adding the Virtual Disk status tray icon to your system tray

1. Start the Virtual Disk Status tray, and then select the **General** tab.
2. Select the **Show icon in System Tray** check box under **Preferences**. The **Virtual Disk Status tray** icon appears in your system tray the next time the target device boots.

vDisks

Use the information in this article to create a base vDisk image.

A vDisk acts as a hard disk for a target device and exists as disk image files on a Citrix Provisioning™ server or on a shared storage device. A vDisk consists of a VHDX base image file, any associated properties files, such as a `.pvp` file and if applicable, a chain of referenced VHDX differencing disks, `.avhdx`.

When creating a vDisk image file, keep the following in mind:

- Create as many vDisk image files as needed, as long as you have enough space available on the provisioning server. Ensure that you have enough available space on the storage device containing the vDisk image files.
- vDisk files use FAT (File Allocation Table) or NTFS (New Technology File System) file systems for Microsoft operating systems.
- Depending upon the file system used to store the vDisk, the maximum size of a VHDX file (vDisk) is 2 terabytes (NTFS) or 4,096 MB (FAT).
- A vDisk can be shared (Standard Image) by one or more target devices, or it can exist for only one target device to access (Private Image).

> **Note:**

The **Cache on hard disk** feature option currently appears in the product but does not function.

The first stage in the lifecycle of a vDisk is creating one. Creating a vDisk requires preparing the master target device for imaging. Once the image is prepared, create and configure a vDisk file where the vDisk resides. Image the master target device to that file. These steps result in a new base vDisk image. This process can be performed automatically, using the Imaging Wizard, or manually. Citrix Provisioning includes an option to create a common image for a single target platform or for use with multiple target platforms.

Note:

Your administrative role determines what information is displayed and tasks performed in the Citrix Provisioning console. For example, view and manage vDisks in sites in which you are a *site administrator*. However, unless the *farm administrator* sets a site as the owner of a store, the site administrator cannot perform store management tasks.

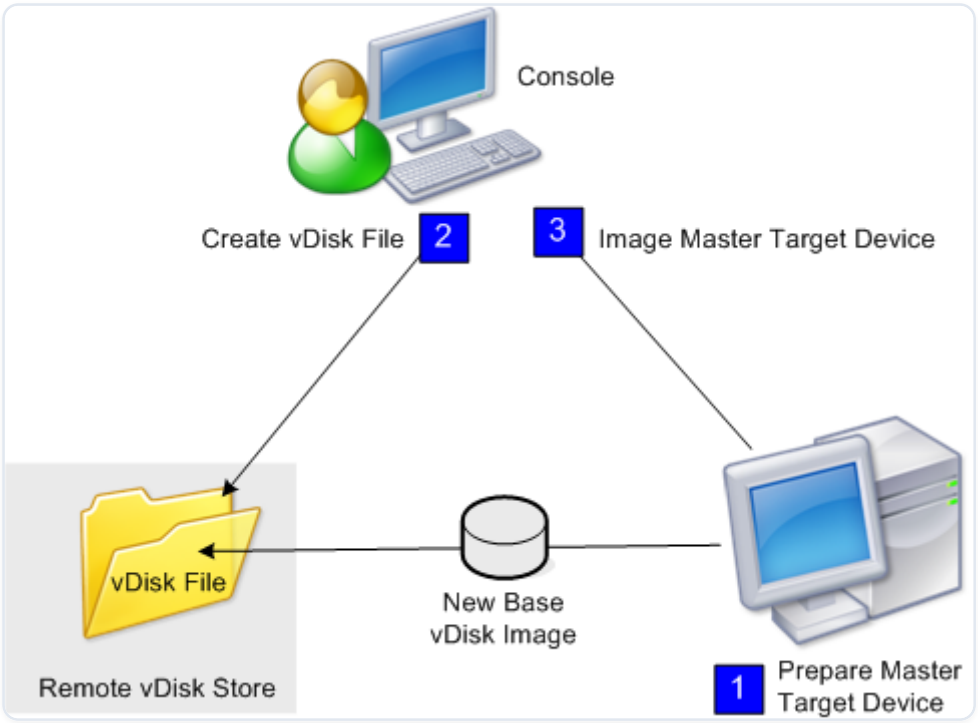
Tip:

Citrix Provisioning only supports automated vDisk capture. More steps require a vDisk attached to the machine being captured, ensuring that a P2PVS switch can be used with P2PVS or the imaging wizard. Use automation steps to accommodate such scenarios.

The following provides an overview of the steps necessary to create a vDisk automatically and manually.

Automatically creating a vDisk image using the imaging wizard

Using the Imaging Wizard is the recommended method for creating vDisk images.



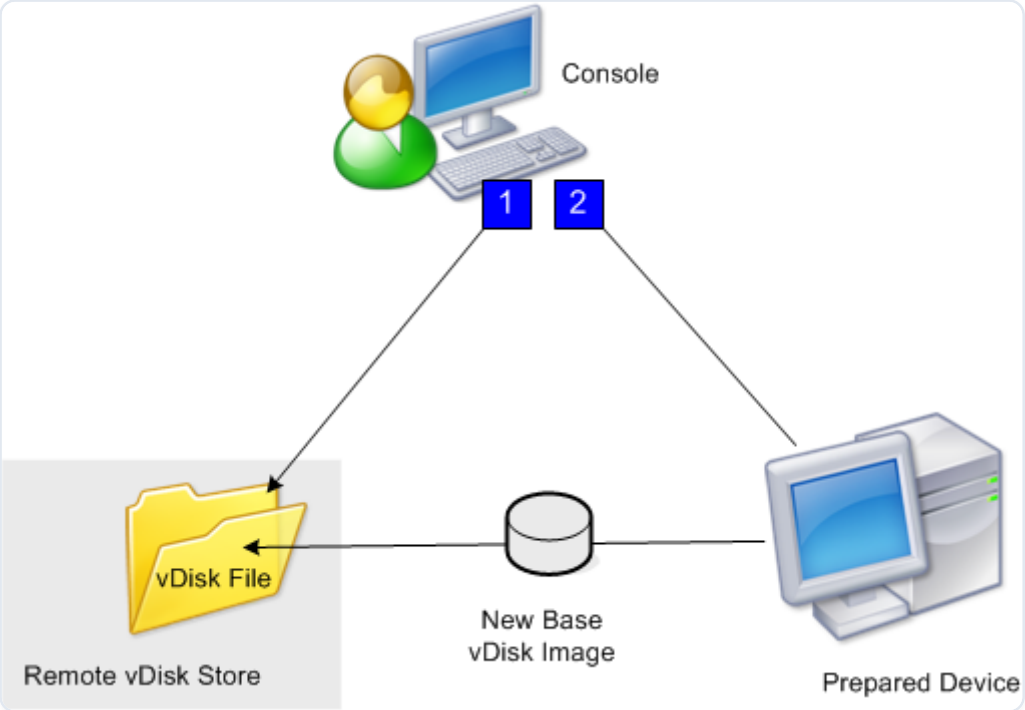
Note:

The master target device, physical or virtual, is prepared by installing and configuring the operating system. Also, configure applications in the base vDisk image. For details, see *Preparing the Master Target Device*.

To image the master target device, run the Imaging Wizard to automatically create a vDisk file on a server or shared storage. After running the Wizard, image the master target device to that file.

Manually creating a vDisk file then creating the image using Citrix Provisioning imaging

This process is the optional method used to create vDisk images.



1. Prepare the master target device, physical or virtual, by installing and configuring the operating system. Prepare applications in the base vDisk image. A vDisk file is then created on a provisioning server or shared storage. Access it using any server providing the vDisk. The file must be mounted, formatted, then unmounted manually using the console or from the target device.

   > **Note:**
   >
   > In the Citrix Provisioning console, a new vDisk file can be created by right-clicking on the **vDisk Pool** or the **Store**, and then selecting the **Create new vDisk menu option**. Once created, vDisks display in the details pane when a site's vDisk pool is selected, or when a store in the farm is selected.

2. The master target device is imaged to the new vDisk file using the Citrix Provisioning imaging utility.

   > **Note:**
   >
   > The imaging utility converts a server or desktop workload from an online physical machine running Windows to a XerServer (formerly Citrix Hypervisor™) virtual machine or provisioned vDisk. The imaging utility converts a server or desktop workload from an

> offline virtual machine or disk, containing any guest operating system, to a XenServer VM.

Creating vDisk files manually

The following procedure describes how to manually create a vDisk file:

1. In the **console** tree, right-click on the **vDisk Pool** in the site where you want to add vDisks, then select the **Create vDisk** menu option. The **Create vDisk** dialog appears.
2. If you accessed this dialog from the site's vDisk pool, in the menu, select the Store where this vDisk resides. If you accessed this dialog from the store, from the menu, select the site where this vDisk is added.
3. In the **Server used to create the vDisk** menu, select the provisioning server that creates the vDisk.
4. Type a file name for the vDisk. Optionally, type a description for this new vDisk in the description textbox.
5. In the **Size** text box, scroll to select the appropriate size to allocate for this vDisk file. If the disk storing the vDisk images is formatted with NTFS, the limit is approximately 2 terabytes. On FAT file systems, the limit is 4,096 MB.
6. In the **VHDX Format** text box, select the format as either **Fixed** or **Dynamic** (2,040 GB for VHDX emulating SCSI; 127 GB for VHDX emulating IDE). If the VHDX format is Dynamic, from the **VHDX block size** menu, select the block size as either 2 MB or 16 MB.
7. Click **Create vDisk**, a progress dialog opens. Depending on the disk size and other factors, it takes several minutes or more to create the vDisk. After the vDisk is successfully created, it displays in the Citrix Provisioning console's details pane and is ready to be formatted.
8. Right-click on the vDisk in the Console, then select **Mount vDisk**. The vDisk icon displays with an orange arrow if mounted properly.

A vDisk image cannot be assigned to, or boot from a target device until that target device exists in the Citrix Provisioning database. After creating the target device, in the **Console**, select the **Hard Disk boot** option.

About the common vDisk image feature

The Common Image feature allows a single vDisk to simultaneously support multiple target device platforms, greatly reducing the number of vDisks an administrator must maintain. The procedure for creating a common image depends on the target device platform.

Supported target device platforms include:

- A combination of XenServer VMs and physical devices (virtual-to-virtual and virtual-to-physical). For details, see vDisks.
- Multiple types of physical devices (different motherboards, network cards, video cards, and other hardware devices). For details, see Creating a Common Image for use with Multiple Physical Device Types.
- Blade servers. For details, see vDisks.

Create common images for use with XenServer® VMs and physical devices, or blade servers

XenServer Platinum Edition enables the provisioning of physical and virtual servers from the same workload image.

Prerequisites:

- Appropriate XenServer Platinum Licensing.
- Support for PXE on the local network.
- DHCP must be installed and configured on the local network.

Select from the following target device platforms:

- Create a common image that boots from a physical or virtual server.
- Create a common image that boots from a blade server.

Create a common image that boots from a physical or virtual server

To create a common image that boots from a physical or virtual machine, complete the procedures as follows.

Prepare the master target device

Install a supported Windows Operating System with the latest patches and device drivers on a physical machine. This physical machine serves as the master target device.

Install the Citrix Provisioning Target Device Software

1. Log on to the master target device as a domain administrator, or a domain user (with local install privileges).
2. Install the Citrix Provisioning server target device software on the physical machine.
3. Follow the onscreen prompts by selecting installation default settings.

4. When prompted, reboot the master target device from the hard disk drive.

Install Citrix VM tools

1. Log on to the master target device as a domain administrator, or a domain user (with local install privileges).
2. Download the Citrix VM tools for Windows installation file `managementagent.msi` from the XenServer downloads page.
3. Run the `managementagent.msi` file to begin Citrix VM Tools installation. The Citrix VM Tools for Windows setup dialog appears.
4. Click **Yes** to continue the install.
5. Follow the onscreen prompts and select the default settings. At the **Choose Install Location** dialog box, click **Install**.
6. When prompted by Windows Plug and Play dialogs, select the option to find drivers automatically.
7. When prompted select **Yes** for any unsigned driver dialog.
8. When prompted, restart the master target device.
9. Verify that Citrix Provisioning successfully binds to the XenServer NIC and the physical systems NIC.

Image the Provisioning Server master target device

Use Citrix Provisioning Imaging Wizard to create the XenServer vDisk image. When creating the vDisk image, you must select to optimize target device settings. Otherwise the VM fails to start.

After successfully creating the XenServer vDisk image, boot both the physical and virtual machines in standard image mode.

For details on using the Citrix Provisioning Imaging Wizard, see Using the Imaging Wizard.

Create a common image that boots from a blade server

To create a common image using the common hard drive method that boots from heterogeneous Blade servers, complete the following steps:

1. Use the Console to create a vDisk file.
2. Log on to the blade server to create a system:

    a. Install the OS on the new machine.

b. Install HP System Pack. This process installs all drivers.

c. Install all necessary Windows updates.

d. Install Citrix Provisioning target device software.

3. PXE boot from the new system's hard disk drive, then verify that the system can recognize the vDisk. The vDisk is shown from "My Computer" as a partition.
4. Physically move the HDD or HDDs in a RAID system to the other system (usually the older system).
5. Boot from the new systems hard disk drive.
6. After Windows installs the driver's, reboot when prompted.
7. Verify that NIC drivers installed correctly.
8. PXE boot from the hard disk drive on the second system.
9. Use Citrix Provisioning Imaging Wizard to create the vDisk image.
10. After imaging completes, shut down the system.
11. Set both systems to boot from the vDisk.
12. On the Citrix Provisioning console, change the vDisk mode to standard cache on local hard disk drive.

Create a common image for use with multiple physical device types

Using the common NIC method, a single vDisk can simultaneously support different motherboards, network cards, video cards, and other hardware devices. The result is a vDisk capable of being used by heterogeneous target devices, greatly reducing the number an administrator must maintain. Use the information in this article to create a common image for physical devices.

Prerequisites

- Make sure all target devices using the common image have a consistent HAL; they must have the same number of logical processors.

> **Tip:**
>
> A single processor, hyper-threading capable system is considered to have two logical processors when hyper-threading is enabled in the UEFI.

- The BIOS structure, presented to the OS during the boot process, must be of the same format for all target devices that share a Standard Image. BIOS structure contains a list of all the components connected to the motherboard so that the appropriate drivers are loaded. This configuration allows the components to function properly.
- Have either a 3Com Managed PC Boot Agent (MBA) or a PXE-compliant NIC available. This card is the common NIC that is inserted into each target device during the Common Image build process.
- Install all the latest device drivers on each target device.
- Device drivers are missing if devices do not respond after you configure the common image. For example, if a target device's USB mouse and keyboard do not respond after you assign the common image to the target device, the drivers for that target device's chipset have not been installed. Go to device manager and check to insure no yellow exclamation mark appears on any devices, especially USB root HUBs and controllers.
- Determine which target device contains the latest motherboard chipset. This target device is used as the first target device in the common image build process. The latest Intel chipset driver contains all the drivers for the previous chipset. It is not necessary to install as many drivers when you build the common image.
- Except on the first target device, disable built-in NICs on all target devices using the common image. Leave the built-in NIC on the first target device enabled. Disabling the NICs prevents confusion about which NIC to use during the common image building process.
- Install Citrix Provisioning components.

Building the common image

To build a common image:

- Configure the master target device
- Export specific data files
- Boot the master target device
- Add extra target devices to the common image

> **Important:**

> When building the common image, create a vDisk that has enough space to accommodate additional information added by the common image build process.

Configuring the master target device

1. Insert the common NIC into the Master Target Device.
2. Install the target device software on the Master Target Device. Select both the common NIC and built-in NICs during the installation process.
3. Create a vDisk, then mount, format, and unmount it. Create a vDisk that has enough space to accommodate additional information added by the common image build process.
4. Run the Imaging Wizard on the target device to build the vDisk.
5. Citrix recommends making a copy of the original vDisk created in Step 3 and save it in the vDisk directory on the provisioning server.
6. On the first target device, copy **CIM.exe** from C:\Program Files\Citrix\Provisioning Services to a removable storage device, such as a USB flash drive. This utility is used to include disparate target devices in the common image.
7. Shut down the Master Target Device and remove the common NIC.

Exporting specific data files

1. Insert the common NIC into a target device added to the common image, then boot the target device from its local hard drive.

   > **Note:**
   >
   > Although the Windows OS must be installed on this target device, the target device software does not have to be installed.

2. Copy **CIM.exe** from the removable storage device to this target device.
3. At a command prompt, navigate to the directory in where CIM.exe is located. Run the following command to extract the information from the target device into the .dat file:

   CIM.exe e targetdeviceName.dat

   where **targetdeviceName** identifies the first target device that uses the common image. For example, TargetDevice1.dat.

   Copy the .dat file created in Step 3 to the removable storage device.
4. Shut down the target device and remove the common NIC.

> **Note:**
>
> To include more target devices with disparate hardware in the common image, repeat this procedure for each device, giving each .dat file a unique name.

Booting the master target device

1. Reinsert the common NIC into the Master Target Device. Insert the NIC into the same slot from which it was removed during the Configuring the Master Target Device procedure. Before booting the Master Target Device, enter the **UEFI setup** and verify that the common NIC is the NIC used in the boot process.
2. Using the common NIC, boot the Master Target Device from the vDisk, in Private Image mode.
3. Copy the `CIM.exe` and the `.dat` file associated with the first target device from the removable storage device to the master target device.
4. At a command prompt, navigate to the directory where the CIM.exe and the .dat file are located.
5. Run the following command to merge the information from the .dat file into the common image:

   CIM.exe m targetdeviceName.dat
6. Shut down the Master Target Device.

Adding more target devices to the common image

1. Insert the common NIC into more target devices included in the Common Image. Insert the NIC into the same slot from which it was removed in the Exporting Specific Data Files procedure.
2. Using the common NIC, boot the target device off the vDisk in Private Image mode.
3. Allow Windows time to discover and configure all the device drivers on the target device. If prompted by the “Found New Hardware Wizard” to install new hardware, cancel the wizard and proceed to Step 4.

   > **Note:**
   >
   > Sometimes, Windows can’t install drivers for the built-in NIC on a target device, and the drivers cannot be installed manually. The common NIC and the target device’s built-NIC are similar to each other. As a result, the driver installation program tries to update the driver for both NICs. For example, if the common NIC is an Intel Pro 100/s and the target

> device's built-in NIC is an Intel Pro 100+. To resolve this conflict, open **System Properties**. On the **Hardware** tab, click the **Device Manager** button. In the **Device Manager** list, right-click the built-in NIC and click **Update Driver** to start the Hardware Update Wizard. Choose **Install** from a list or specific location and specify the location of the NIC's driver files.

4. Open **Network Connections**. Right-click the connection for the built-in NIC and click **Properties** in the menu that appears. The icon for the built-in NIC is marked with a red X.
5. Under **This connection uses the following items**, select **Network Stack** and click **OK**.
6. From a command prompt, run the following command:

   ```
   C:\Program Files\Citrix\Provisioning Server\regmodify.exe
   ```

   > **Note:**
   >
   > After completing Steps 4–6, reboot the target device and allow Windows to discover and configure any remaining devices. If prompted by the "Found New Hardware Wizard" to install new hardware, proceed through the Wizard to complete the hardware installation.

7. Using the original vDisk, repeat Step 1 through Step 6 for each of the additional target devices you want to include in the Common Image.
8. Once target devices have been included in the **Common Image**, open the **Console**. Set the disk access mode for the Common Image vDisk to **Standard Image** mode, then boot the devices.

Deployments using Device Guard

Device Guard represents a combination of enterprise and software security features. It can be used to provide a highly secure environment which allows you to configure systems so that only trusted applications can be used. See the Microsoft site for more information about Device Guard deployments.

When using Device Guard, consider the following:

- Device Guard is a property of an individual VM. This functionality is configured on the Hyper-V host where the VM resides, after the VM is created.

- Enable Device Guard in the master image prior creating the image. Once enabled, you can image the vDisk.

Also:

- See the Microsoft documentation site to configure Device Guard.
- See the Microsoft documentation site to configure nested virtualization.
- Once the vDisk is created, use the Citrix Virtual Apps and Desktops™ Setup Wizard to provision the VMs.
- Once the VMs are provisioned, manually enable nested virtualization for each VM on the Hyper-V host on which it has been provisioned.

Citrix Provisioning supports the following enabled with Device Guard using Hyper-V 2016 and newer, or ESX 6.7 and above:

- Targets running on Windows 10, Windows 2016, or Windows 2019.
- Citrix Provisioning server on Windows Server 2016, 2019, or 2022.

Consider also the following restrictions for Hyper-v 2016 in a Citrix Provisioning target device:

- The hyper-v network must not be created if the client is running one NIC.
- The hyper-v network can be created using any other NICs other than the streaming NIC.

Configuring vDisks for Active Directory management

Integrating Citrix Provisioning™ and Active Directory allows administrators to:

- Select the Active Directory Organizational Unit (OU) for the Citrix Provisioning target device computer account.
- Take advantage of Active Directory management features, such as delegation of control and group policies.
- Configure the Citrix Provisioning server to automatically manage the computer account passwords of target devices.

Before integrating Active Directory within the farm, verify that the following prerequisites are met:

- The master target Device was added to the domain before building the vDisk.
- The **Disable Machine Account Password Changes** option was selected when the running the image optimization wizard.

After all prerequisites have been verified, new target devices can be added and assigned to the vDisk. A machine account is then created for each target device.

Tip:

Running the PowerShell command `Add-PvsDeviceToDomain` without specifying a parameter adds all targets in every site to the computer's container in Active Directory.

Managing domain passwords

When target devices access their own vDisk in Private Image mode, there are no special requirements for managing domain passwords. However, when a target device accesses a vDisk in standard image mode, the provisioning server assigns the target device its name. If the target device is a domain member, the name and password assigned by the server must match the information in the corresponding computer account within the domain. Otherwise, the target device is not able to log on successfully. For this reason, the provisioning server must manage the domain passwords for target devices that share a vDisk.

To enable domain password management you must disable the Active Directory-(or NT 4.0 Domain) controlled automatic renegotiation of machine passwords. This process is done by enabling the Disable machine account password changes security policy at either the domain or target-device level. The provisioning server provides equivalent functionality through its own **Automatic Password Renegotiate** feature.

Target devices booted from vDisks no longer require Active Directory password renegotiation. Configuring a policy to disable password changes at the domain level applies to any domain members booting from local hard drives. If policies disabling password changes are not desirable for your environment, disable machine account password changes at the local level. To disable machine account password changes, select the **Optimize** option when building a vDisk image. The setting is applied to any target devices that boot from the shared vDisk image.

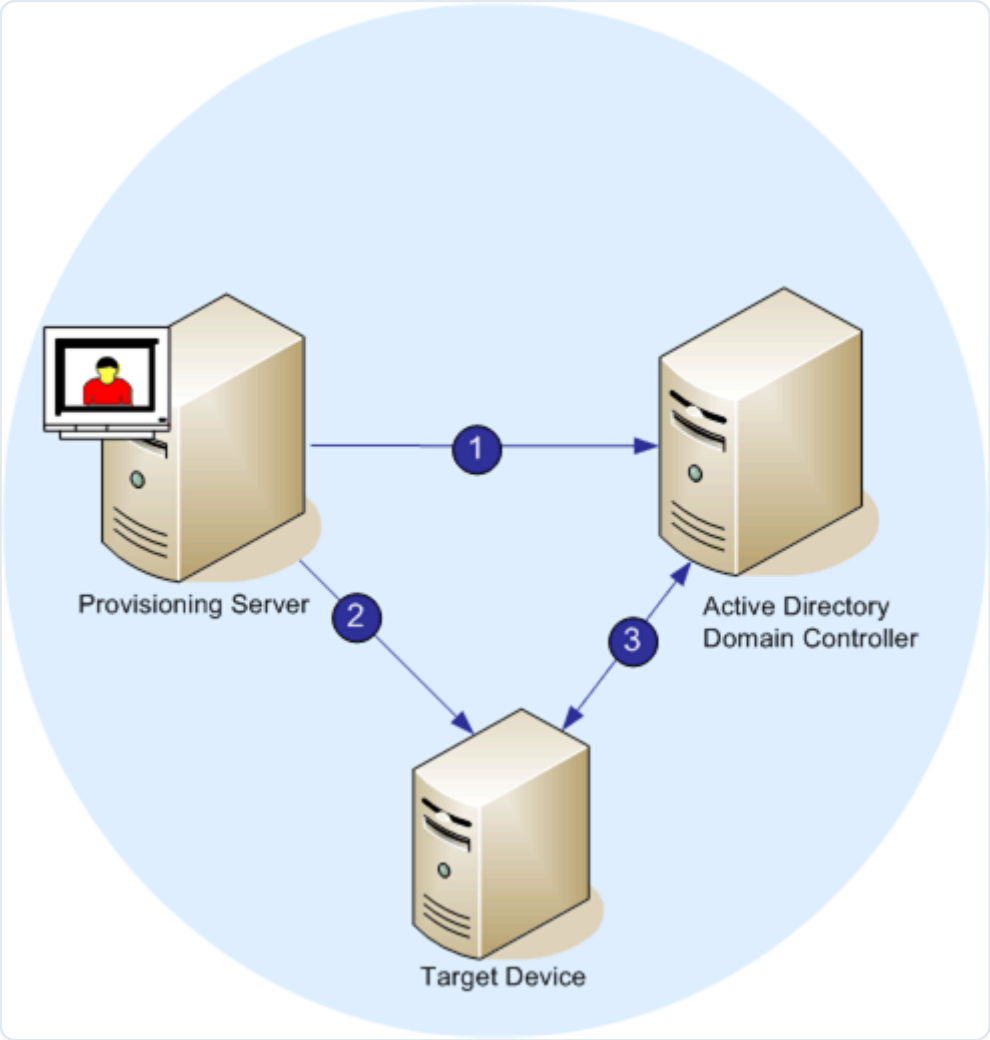
Note:

The Citrix Provisioning server does not in any way change or extend the Active Directory schema. The provisioning server’s function is to create or modify computer accounts in Active Directory, and reset passwords.

> When domain password management is enabled, it:

- Sets a unique password for a target device.
- Stores that password in the respective domain computer account.
- Gives the information necessary to reset the password at the target device before it logs on to the domain.

Password management process



With password management enabled, the domain password validation process includes:

- Creating a machine account in the database for a target device, then assign a password to the account.
- Providing an account name to a target device using the Streaming Service.
- Having the domain controller validate the password provided by the target device.

Enabling domain management

Each target device that logs on to a domain requires a computer account on the domain controller. This computer account has a password maintained by the Windows desktop OS and is transparent to the user. The password for the account is stored both on the domain controller and on the target device. If the passwords stored on the target device and on the domain controller do not match, the user cannot log on to the domain from the target device.

Domain management is activated by completing the following tasks:

- Enabling Machine Account Password Management
- Enabling Automatic Password Management

Enabling machine account password management

To enable machine account password management, complete the following:

1. Right-click on a vDisk in the Citrix Provisioning console, then select the **File Properties** menu option.
2. On the **Options** tab, select **Active Directory machine account password management**.
3. Click **OK**, then close the properties dialog, then restart the Streaming Service.

Enabling automatic password management

If your target devices belong to an Active Directory domain and are sharing a vDisk, complete the following extra steps.

To enable automatic password support, complete the following:

1. Right-click on a provisioning server in the console, then select the **Properties** menu option.
2. Select the Enable automatic password support option on the **Options** tab.
3. Set the number of days between password changes.
4. Click **OK** to close the **Server Properties** dialog.
5. Restart the Streaming Service.

Managing domain computer accounts

The tasks documented here must be performed using the Citrix Provisioning server, rather than in Active Directory, to take full advantage of product features.

Supporting cross-forest scenarios

To support cross-forest scenarios:

- Ensure that the DNS is properly set up. See the Microsoft website for information on how to prepare DNS for a forest trust.
- Ensure the forest functional level of both forests is the same version of Windows Server.
- Create the forest trust. To create an account in a domain from another forest, create an Inbound Trust from the external forest to the forest where Citrix Provisioning resides.

Parent-child domain scenario

Common cross-domain configurations involve having the Citrix Provisioning server in a parent domain with users from one or more child domains. These users can administer Citrix Provisioning and manage Active Directory accounts within their own domains.

To implement this configuration:

1. Create a Security Group in the child domain; it can be a *Universal*, *Global*, or *Local Domain Group*. Make a user from the child domain a member of this group.
2. From the provisioning server console, in the parent domain, make the child domain security group a Citrix Provisioning Administrator.
3. If the child domain user does not have Active Directory privileges, use the Delegation Wizard in the **Active Directory Users & Computers Management Console**. Use this method to assign, create, and delete a user's computer account rights for the specified OU.
4. Install the Citrix Provisioning Console in the child domain. No configuration is necessary. Log in to the provisioning server as the child domain user.

Cross-forest configuration

This configuration is similar to the cross-domain scenario. However, in this configuration the Citrix Provisioning console, user, and administrator group are in a domain that is in a separate forest. The steps are the same as for the parent-child scenario, except that a forest trust must be established first.

> **Note:**
>
> Microsoft recommends that administrators do not delegate rights to the default Computers container. The best practice is to create accounts in the OUs.

Giving access to the Provisioning Console for users in another domain

The groups for administrative roles are limited to groups in the native domain and domains with a two-way trust to the native domain. When granting access, consider:

- **Domain1** represents the domain containing the Provisioning Server and service accounts.
- **Domain2** represents the domain with a two-way trust to **Domain1**. It contains the user accounts which were granted access to the Provisioning Console.

To grant Provisioning Console access to users from another domain:

1. Create a Domain Local Group in **Domain2**, and add the user account to this group.
2. Log in to the Provisioning Console using an existing administrator account.
3. Click **Farm Properties**. Select the **Groups** tab.
4. In the Domain drop-down menu, choose **Domain2**.
5. Retain the * to view all the groups associated with **Domain2**, or filter the groups by entering then the name of the Group you want to add. Click **Search**.
6. Select the group by clicking the associated checkbox. Click **Add**.

Adding target devices to a domain

> **Note:**
>
> The machine name used for the vDisk image must not be used again within your environment.

1. Right-click on one or more target devices in the Console window. You can alternatively right-click on the device collection itself to add all target devices in this collection to a domain. Select **Active Directory**, then select **Create machine account**. The **Create Machine Accounts in Active Directory** dialog appears.
2. From the **Domain** combo box, select the domain that the target device belongs to or type the domain name.
3. From the Organization unit (OU) scroll list, select, or type the organization unit to which the target device belongs. The syntax is ‘parent/child,’ lists are comma separated. If nested, the parent goes first.
4. Click **Create Account** to create the account in the selected domain. Click **Close** to exit the dialog.

Removing target devices from a domain

1. Right-click on one or more target devices in the console window. Alternatively, right-click on the device collection itself to add all target devices in this collection to a domain. Select **Active Directory**, then select **Delete machine account**. The **Delete Machine Accounts from Active Directory** dialog appears.
2. In the **Target Device** table, highlight those target devices that you want to remove from the domain, then click **Delete Account**. Click **Close** to exit the dialog.

Reset computer accounts

> **Note:**
>
> An Active Directory machine account can only be reset when the target device is inactive.

> To reset computer accounts for target devices in an Active Directory domain:

1. Right-click on one or more target devices in the Console window. Alternatively right-click on the device collection itself to add all target devices in this collection to a domain. Then select **Active Directory**, then select **Reset machine account**. The **Reset Machine Accounts Passwords in Active Directory** dialog appears.
2. In the **Target Device** table, highlight those target devices to reset, then click **Reset Account**.
3. Click **Close** to exit the dialog.
4. Disable Windows Active Directory automatic password renegotiation. To disable automatic password renegotiation on your domain controller, enable the following group policy: Domain member: Disable machine account password changes.

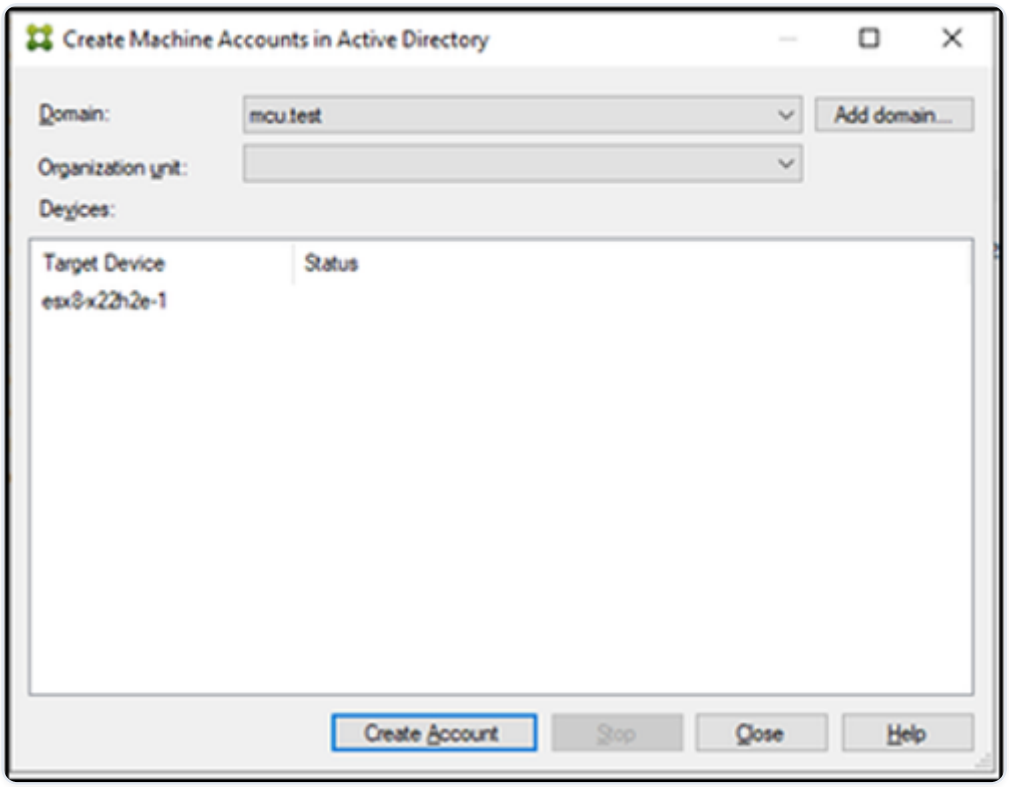
   > **Note:**
   >
   > To make this security policy change, you must have sufficient permissions to add and change computer accounts in Active Directory. You have the option of disabling machine account password changes at the domain level or local level. If you disable machine account password changes at the domain level, the change applies to all members of the domain. If you change it at the local level (by changing the local security policy on a target device connected to the vDisk in Private Image mode), the change applies only to the target devices using that vDisk.

5. Boot each target device.

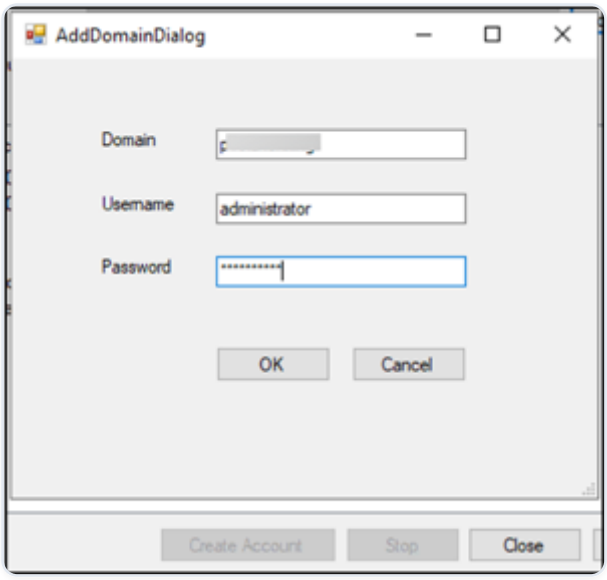
Adding untrusted domains to the domain list

Citrix Provisioning supports provisioning of target devices in untrusted domains. To add an untrusted domain to the domain list, you must provide valid credentials. If the credentials are valid, the untrusted domain is added to the domain list. You can then create, delete, or reset accounts in Active Directory within the selected domain. To add an untrusted domain:

1. Click **Add domain..**

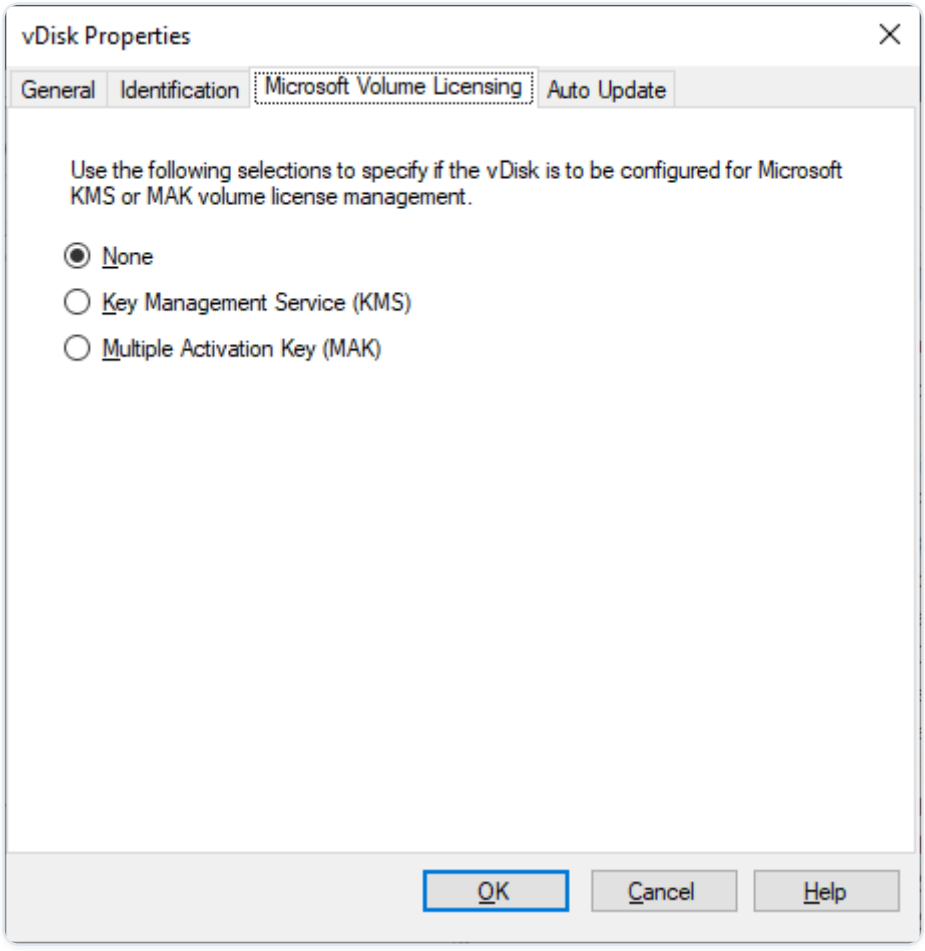


2. In the **AddDomainDialog**, enter the domain name, username, and password for the untrusted domain.



Active directory-based activation

Update how Microsoft Volume Licensing is configured for an individual vDisk using Active Directory-based activation. With this functionality you can specify that the vDisk uses no volume licensing.



Note:

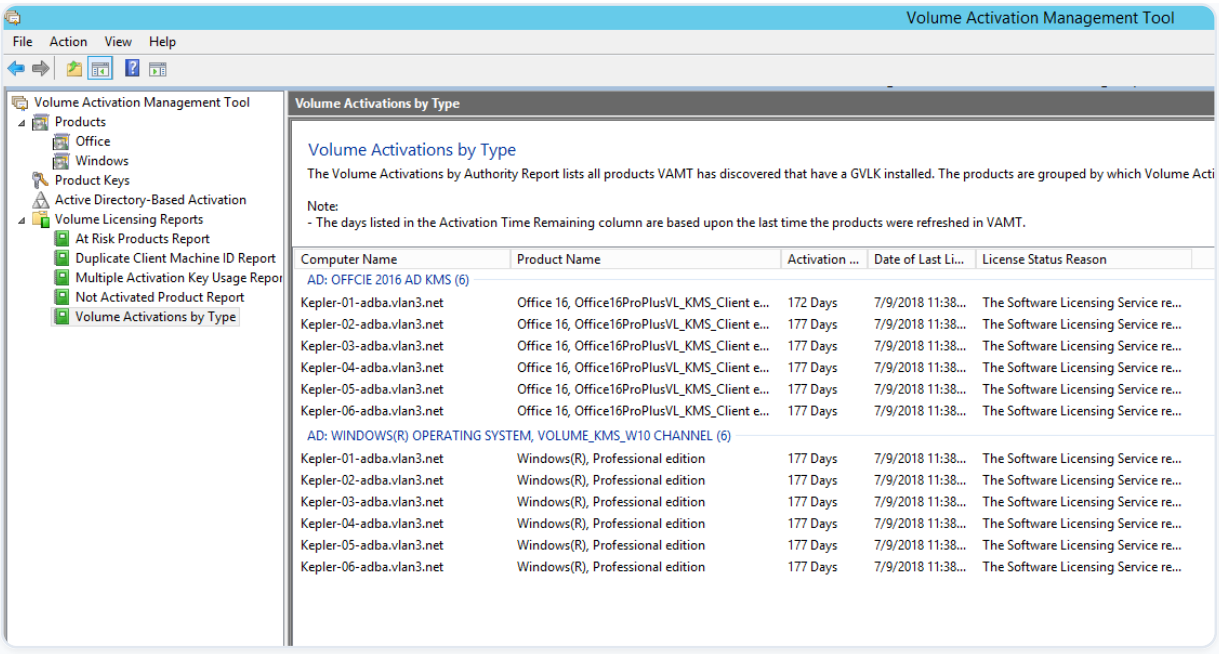
When using the Microsoft Volume Licensing for a vDisk, consider that Key Management Services (KMS), Multiple Activation Key (MAK) and Active Directory-based activation (ADBA) cannot be used together.

To improve active directory-based activation:

1. In the vDisk Property screen, set the vDisk Microsoft Licensing property to **None**.
2. On the target device, use `slmgr-dlv` for a Microsoft image, and `cscript ospp.vbs/dstatus` for a Microsoft Office image.

Tip:

A known issue exists where VAMT displays errors about duplicate CMID entries for ADBA activated devices. This issue occurs although ADBA does not use CMID. ADBA, despite being similar to KMS, does not use CMID. Microsoft reuses KMS data when compiling CMID information. The following image illustrates a VAMT tool screen for ADBA. The **Volume Activation by Type** screen displays conflicts for duplicate CMID entries for those devices.



Assigning vDisks to target devices

Assign a vDisk to a single target device or to all devices within a target device collection. If a target device has more than one vDisk assigned to it, a list of disks appears at boot time. This process allows you to select the appropriate vDisk to boot.

If one or more vDisk versions exist, the version target devices use in Production is either the highest numbered production version or an override version. For details see Accessing a vDisk Version. Maintenance and Test devices with non-production versions are labeled appropriately.

Assigning vDisks to a target device

vDisks can be assigned to a single target device using:

- Drag
- Target Device Properties dialog

To assign a vDisk, using drag, to one or all target devices within a collection:

1. In the Citrix Provisioning™ console tree, expand the vDisk Pool within a given site. Or, alternately expand **Stores** to display the assigned vDisk in the right pane of the window.
2. Left-click and hold the mouse on the vDisk, then drag it onto the target device or onto the collection.

To assign one or more vDisks to a single target device from the **Target Device** Properties dialog:

1. In the Citrix Provisioning console tree, expand the **Device Collections** folder, then click the collection folder where this target device is a member. The target device displays in the details pane.
2. Right-click on the target device, then select **Properties**. The **Target Device Properties** dialog appears.
3. On the **General** tab, select the boot method that this target device uses from the **Boot from** menu options.
4. On the vDisks tab, select the **Add** button within the vDisk for this Device section. The **Assign vDisks** dialog appears.
5. To locate assignable vDisks for this target device, select a specific store or server. These stores or servers are located under the Filter options. You can alternately accept the default setting, which includes **All Stores** and **All Servers**.
6. In the **Select the desired vDisks** list, highlight the vDisk(s) to assign, then click **OK**, then **OK** again to close the **Target Device Properties** dialog.

Citrix Provisioning™ on Microsoft Azure

This article explains how to move your Citrix Provisioning workloads to the Azure Cloud, using the same provisioning tools and policies as you use with on-premises hypervisors.

This functionality includes support for the Citrix Virtual Apps and Desktops™ Setup Wizard. You can integrate with Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) using the same tools that you already know. Installing Citrix Provisioning in your Azure subscription is the same as installing it in an on-premises provisioning farm.

Supported features

The following Citrix Provisioning features are supported when provisioning workloads in Azure:

- UEFI boot of Generation 2 Azure VMs using BDM boot partition.
- Streaming 64-bit Windows 10, Windows 11 (Standard Security Type only), Windows 11 22H2, and Windows Server 2016/2019/2022 target VMs
- The Citrix Virtual Apps™ and Desktops Setup wizard to provision target VMs and add them to Citrix DaaS catalog.
- The import wizard lets you import manually provisioned VMs into the provisioning server.
- The export wizard lets you create and update catalogs in Citrix DaaS™ from manually provisioned targets.
- Create a master VM in Azure to act as the source of the virtual disk (vDisk) to be used by the provisioning server.
- Create a vDisk from an Azure master VM and update it using either provisioning versioning, or reverse imaging.
- Import an existing image to your Azure setup using the Citrix Image Portability Service. See Citrix IPS.
- Power management of targets from Citrix DaaS, provisioning console, Azure Portal, and Azure APIs.
- Azure SQL Database
- Azure SQL Managed Instance
- Active Directory support using one of the following:
    - Integrating with an on-premises forest by installing domain controller VMs in Azure and connecting them to the on-premises forest through an ExpressRoute connection. You can

connect your on-premise AD infrastructure to your AAD tenant via the Microsoft AD Connect feature.

  - Implementing a standalone Active Directory domain in Azure by installing and configuring domain controller VMs in Azure.
  - Azure AD Domain Services can provide an AD environment that Citrix Provisioning can use. You can synchronize your on-premises forest with your Azure AD tenant using AD Connect to provide a fully integrated solution.

- Create targets in specific availability zones. To do this:

  a. For each availability zone that the targets will use, create a template VM located in that zone.

  b. Run the Citrix Virtual Desktops™ Setup Wizard for each zone using the template for that zone.

Limitations

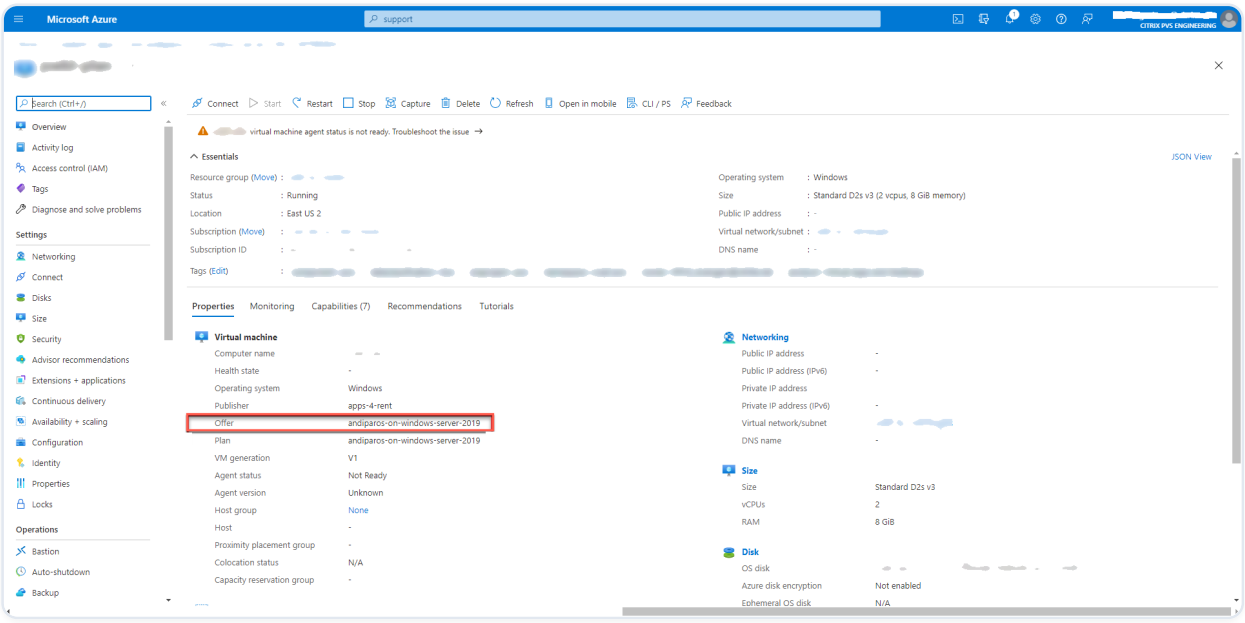
The following features are not supported:

- 32-bit operating systems.
- Windows Server 2012 and earlier are not supported.
- Secure boot and trusted launch are not currently supported.
- PXE and ISO boot of master and target VMs, because Azure does not support them.
- Generation 1 (BIOS) VMs. Only Generation 2 (UEFI) VMs are supported.
- Streamed VM Setup Wizard.
- vDisk Update Management.
- Virtual Host Connection Wizard.
- Auto-Add Wizard.
- Removal of VMs, catalogs, or AD accounts from Citrix Provisioning console is not supported when Citrix Provisioning is integrated with customer-managed Delivery Controller.
- The Citrix Provisioning API, which provides scripted access to the provisioning process, is not supported.
- The Azure machine size used when creating the master VM must be compatible with that used when creating target VMs. Only Generation 2 VMs are supported. This includes the following:

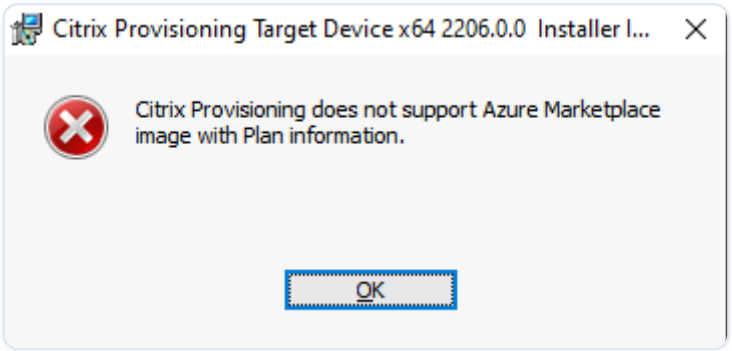
  - Presence or absence of a temporary disk must be the same

  - Presence or absence of a GPU must be the same

- Template VMs (VMs to be used as a template for creating targets) must exist in the region associated with Citrix DaaS hosting unit. Therefore, for this release you have to create a template VM in each region.
- The Azure disks created for the boot and cache disks of target VMs are of type Standard SSD. Currently, this setting cannot be changed.
- You cannot use pay-as-you-go marketplace image.



If you try to create vDisks from master VMs that have plan information, creation will fail with the following error message:



Consider the following Azure limitations:

- No more than 2500 VMs can be created in a single subscription.
- If you plan to use Azure File Services to provide storage for vDisks, you must create a Premium Storage Account.

Requirements

To use Citrix Provisioning on Azure you need the following:

- System requirements for the on-premises version of the product.
- License for this latest version of Citrix Provisioning.
- A license server installed.
- An Azure subscription.
- You can have the database on one of the following:
  - Azure SQL Database
  - Azure SQL Managed Instance
  - SQL Server or SQL Server Express on a VM installed in your subscription.
- Citrix Virtual Apps and Desktops Cloud connector VMs installed in your Azure subscription. A separate resource location (set of Cloud Connectors) is required for each combination of subscription+region to be used. Citrix Provisioning supports working with both customer managed and Citrix Cloud™ Delivery Controllers natively from the same Citrix Provisioning Console.

Licensing

The initial product uses the existing licensing mechanism for provisioning. Refer to the Product Setup to access the license server installed in the test subscription for all internal users. Use one of the following licenses:

- If you have a Citrix DaaS subscription, then use the included **Cloud** provisioning license.
- If you have a Citrix Virtual Apps and Desktops license with Hybrid Rights, then you can use this license directly.
- If you do not have either of these, then contact your Citrix® representative to get a suitable trial license.

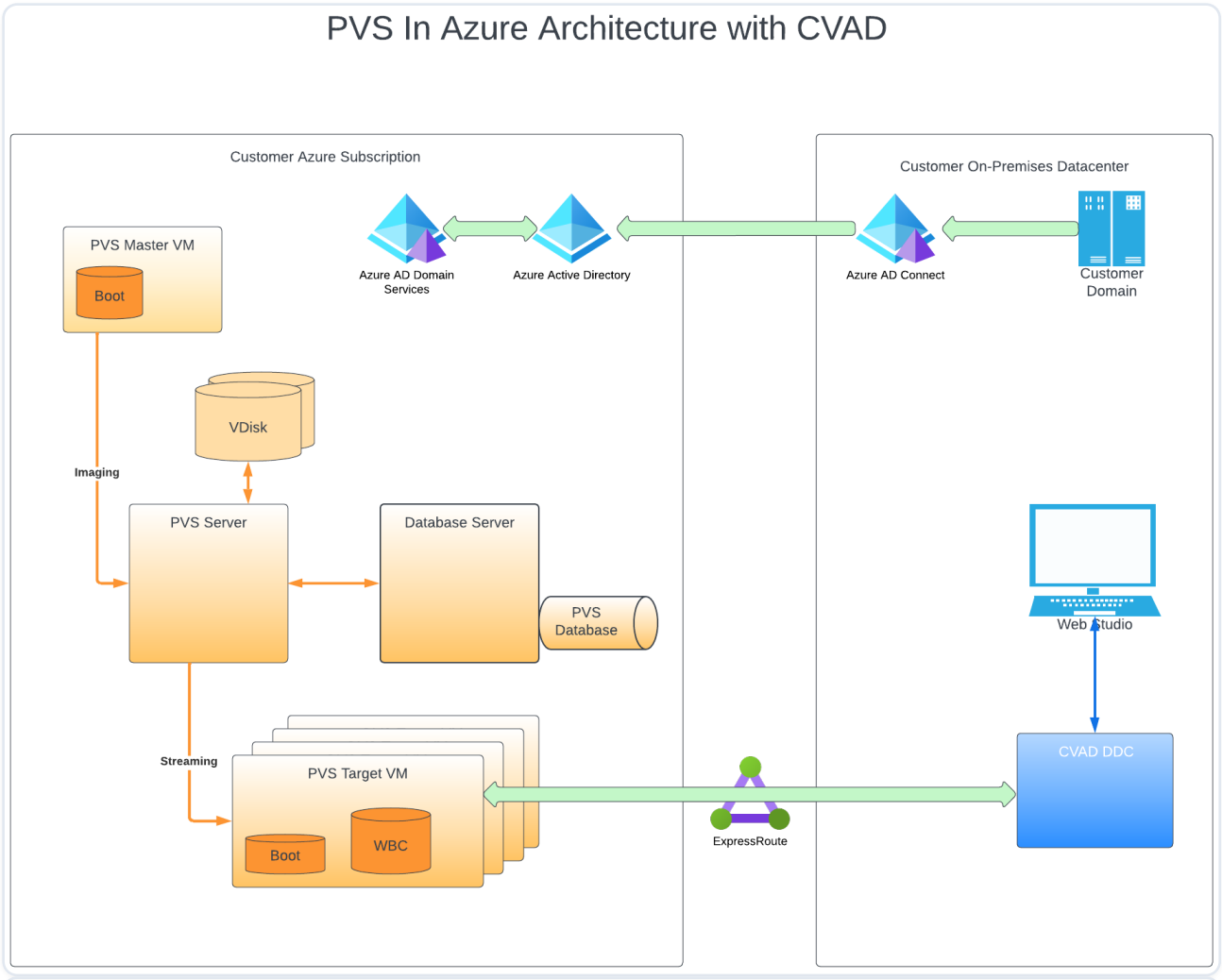
You can install the license server on one of the Citrix Provisioning Server VMs.

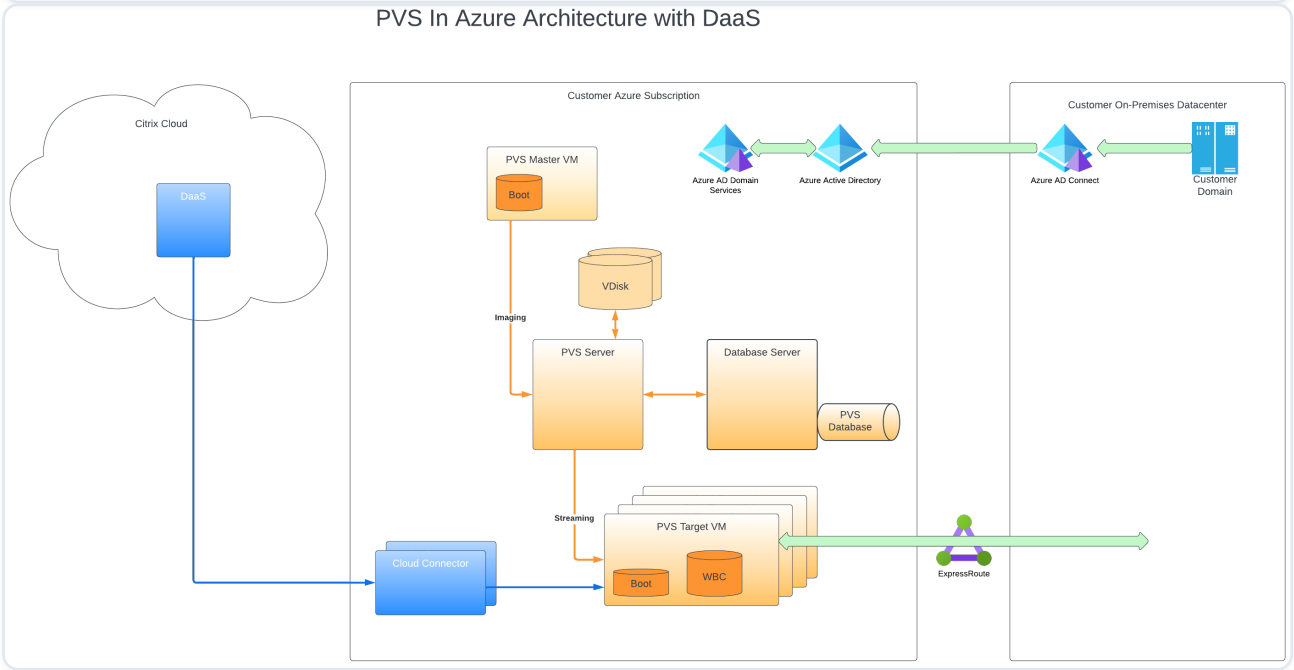
Architecture

This high-level architecture diagram shows the components that are either required or recommended to set up Citrix Provisioning on Azure with:

- Citrix Virtual Apps and Desktops

- Citrix DaaS





This section describes the main components.

Citrix Cloud

When using Citrix Provisioning on Azure, Citrix DaaS, including the:

- Connection Broker
- Connection Broker Catalogs that reference Citrix Provisioning Target VMs running on Azure.

The Citrix Provisioning Server does not manage power for Azure target VMs although targets can be manually turned on and off from the provisioning console. The Broker initiates power management by talking directly to Azure. As the VM boots, it streams the boot disk from the virtual disk maintained by the Citrix Provisioning Server.

Azure Active Directory Classic version

Citrix Provisioning on Azure supports "Classic" Active Directory only. You can make the classic Active Directory available on Azure in one of the ways as described in Set up Active Directory.

Azure database services

Citrix Provisioning supports the following databases:

- SQL Server
- SQL Server Express
- Azure SQL Database
- Azure SQL Managed Instance

The following table lists the Citrix Provisioning version and the supported hypervisors for using Azure SQL Database and Azure SQL Managed Instance.

SUPPORTED CLOUD DATABASE	COMPATIBLE CITRIX PROVISIONING VERSION	COMPATIBLE HYPERVISORS
Azure SQL Database and Azure SQL Managed Instance	2203 and later	Azure
Azure SQL Database	2203 CU2 and later	All supported Citrix Provisioning on-premises hypervisors and cloud hypervisors other than GCP

See Supported authentication types for more information on the supported authentication types. Select the authentication type that best suits your needs.

Hybrid Azure AD

Citrix Provisioning on Azure supports Hybrid Azure AD. For information, see Create Hybrid Azure AD joined catalogs.

Citrix Provisioning Server

You install the Citrix Provisioning Server on a server-class Azure VM, similar to on-premises deployments.

The usual processes for providing storage for vDisks apply:

- You can use local storage on the server VM and manage replication of vDisks between servers yourself.
- Use Azure Files to provide an SMB server that can be accessed from any server in the region to create a Premium Storage account to host Azure Files. It is only supported for access in the same region as the provisioning server.

> **Tip:**
>
> The storage account must be premium.

- Create a separate VM to act as a file server for sharing vDisks.

Target VMs boot using a small boot disk

The Citrix Provisioning Server and targets do not support either PXE or ISO boot, because they are not available on Azure. Instead, target VMs boot uses a small boot disk, the BDM Boot Disk, which is about 20 MB and contains the Citrix Provisioning UEFI boot application.

Once the BDM app is running, it uses the Citrix Provisioning protocol to stream the virtual disk contents to the VM. The Citrix Virtual Apps and Desktops Setup Wizard can be used to create BDM boot disk. If you want to manually provision target VMs, you can use the BDM.exe tool to create a VHD file. This file is the boot image which can then be uploaded to Azure.

Provisioning of target VMs

The Citrix Virtual Apps and Desktops Setup Wizard can handle all the required steps for provisioning target VMs including:

- Creation and upload of the boot disk including configuration of provisioning servers to contact.

- Creation of Active Directory computer accounts, or import of existing computer accounts.
- Creation of the target VM including the network connection, the boot disk, and Citrix Provisioning WBC disk to hold the cache.
- Configuring the provisioned targets in the provisioning server database.
- Initial boot and shutdown of the target VMs to enable the WBC disk to be formatted.
- Creation of a Citrix Virtual Apps and Desktops catalog and adding the provisioned targets to it.

Citrix Provisioning master VM used to capture a virtual disk

The Citrix Provisioning master VM is used to capture a virtual disk. You create the VM manually on Azure where you install the Citrix Provisioning Target Driver package.

The mechanisms for this and the subsequent capture of a virtual disk from the master VM are essentially the same as for existing on-premises installations. There are some important points to note that are covered in the following sections.

Set up Citrix Provisioning on Azure

This section explains the pre-installation tasks, steps for creating a Citrix Provisioning collection with a set of targets streamed from your virtual disk, and links to the Azure docs to guide you.

To set up Azure provisioning, begin by configuring your provisioning server and other infrastructure on Azure. Using the Azure Resource Manager APIs and the instructions, set up the components along the same lines as your current on-premises setup. You can create PowerShell scripts to automate the process.

Pre-installation tasks

Complete the following tasks before installing and configuring Citrix Provisioning.

Select and configure the database

Each Citrix Provisioning farm has a single database. You can provide the database on either:

- A new or existing SQL Server or SQL Server Express Instance.
- A new or existing Azure SQL Database server.
- A new or existing Azure SQL Managed Instance.

All Citrix Provisioning servers in a farm must be able to communicate with the database server.

In a production environment, to avoid poor distribution during load balancing, best practice is to install the SQL Server or SQL Server Express instance and the Citrix Provisioning server component software on separate servers.

There are three ways to create the database:

- Use the Configuration Wizard. To use this option, you need `dbcreator` permission.
- If you do not have permission to create databases, use the **DbScript.exe** utility to create a SQL script that a database administrator can run to create the provisioning database. This utility is installed with the provisioning software.
- If the database administrator creates an empty database by running the DbScript.exe utility, then this database is chosen as the database for the new farm when running the configuration wizard. The login used when running the Configuration Wizard must be the owner of the database. Also, this login must have the **View any definition** permission. The database administrator sets this permission when the empty database is created.

Run the DbScript.exe utility to create or update the database

If you do not have permission to create databases, use **DbScript.exe** to generate a SQL script for the database administrator to run to create or update the PVS database. Run the script from the Windows command prompt in `C:\Program Files\Citrix\Provisioning Services`.

To generate a script to create the database, use this syntax:

- For SQL Server, SQL Server Express, or Azure SQL Managed Instance: `DbScript.exe -new <databaseName> <farmName> <siteName> <collectionName> <farmAdminGroup> <adGroupsEnabled> <scriptName> <is2012orHigher>`
- For Azure SQL Database: `DbScript.exe -newForAzSqlDb <databaseName> <farmName> <siteName> <collectionName> <farmAdminGroup> <adGroupsEnabled> <scriptName> <is2012orHigher>`

When creating a new database for Azure SQL Database, DbScript produces two script files instead of one.

- The first is run into the master database, and it creates the new database.
- The second script is then run into the new database.

This is due to limitations of Azure SQL Database.

To generate the script to update the database, enter:

```
DbScript.exe -upgrade <databaseName> <scriptName>
```

The commands use these arguments:

- `<databaseName>` — Name of the database to create or update.
- `<farmName>` — Farm name for the new database.
- `<siteName>` — Site name for the new database.
- `<collectionName>` — Collection name for the new database
- `<farmAdminGroup>` — Farm administrator group, specified as a full path.

> **Note:**
>
> When you run the configuration wizard, you must be a member of this group (an Active Directory group) to add the PVS servers to the database.

- `<adGroupsEnabled>` — Enable or disable AD groups, specified as Boolean, where `true` enables AD groups and `false` disables AD groups.
- `<scriptName>` — Name of the script to generate, specified as a full path.
- `<is2012orHigher>` — It is deprecated. Always use `true`.

Supported authentication types

Citrix Provisioning on Azure supports more authentication modes to benefit from the features found in Azure SQL Database and Azure SQL Managed Instance. Choose the authentication mode that best suits your needs.

The authentication modes that the Citrix Provisioning on Azure supports are:

- Active Directory Integrated
- SQL Server
- Active Directory Password
- Active Directory Service Principal
- System-Supplied Managed Identity
- User-Supplied Managed Identity

Following are the tables that provide information about the users to which the authentication modes grants access, required credentials, and supported database platforms.

AUTHENTICATION MODE	GRANTS ACCESS TO	REQUIRED CREDENTIALS	NOTE
Active Directory Integrated	Active Directory User	Nothing (uses the current login context)	Create the user name in the Active Directory if you do not want to use an existing one.
SQL Server	SQL Login	Login and Password	Create the SQL login on the database server if you do not want to use an existing one.
Active Directory Password	Active Directory User	Domain-Qualified User name and Password	Create the user name in the Active Directory if you do not want to use an existing one.
Active Directory Service Principal	Application	Name of Application ID, Application ID, Tenant ID, and Secret	Create the registered application in the Active Directory if you do not want to use an existing one. You can generate a new app secret for an existing registered application if you do not want to use an existing secret.
System-Supplied Managed Identity	Virtual Machine	Nothing (uses the current VM)	
User-Supplied Managed Identity	Virtual Machine	Managed Identity Name, Client ID, and Object ID	

AUTHENTICATION MODE	DATABASE PLATFORM
Active Directory Integrated	SQL Server
	Azure SQL Database
	Azure SQL Managed Instance
SQL Server	SQL Server
	Azure SQL Database
	Azure SQL Managed Instance
Active Directory Password	Azure SQL Database
	Azure SQL Managed Instance
Active Directory Service Principal	Azure SQL Database
	Azure SQL Managed Instance
System-Supplied Managed Identity	Azure SQL Database
	Azure SQL Managed Instance
User-Supplied Managed Identity	Azure SQL Database
	Azure SQL Managed Instance

OTHER RESTRICTIONS

- Restrictions on Active Directory Integrated authentication:
  - With SQL Server: The Citrix Provisioning server must belong to a domain, the provisioning service user context must be a domain user, and Citrix Provisioning must be configured by a domain user.
  - With Azure SQL: Use this authentication mode with Azure SQL, but only from an enterprise domain federated to the Azure tenant domain. The Citrix Provisioning server virtual machine must belong to the enterprise domain, provisioning service account user context must be an enterprise user, and Citrix Provisioning must be configured by an enterprise user. Setting up federated domains is a significant task. Use this option if you have done this earlier. Instead, use **Active Directory Password** authentication.

- Restrictions on System-Supplied Managed Identity authentication:
  - Enable the system assigned managed identity on the Citrix Provisioning server VM.
- Restrictions on User-Supplied Managed Identity authentication:
  - Create a user assigned managed identity or select an existing one, and add that user assigned managed identity to the Citrix Provisioning server VM.

Configuration wizard user permissions

You must have the system privilege of a local administrator to run the configuration wizard.

The **admin database principal** is the database principal used by the configuration wizard to create and set up the provisioning database. The authentication credentials that you specify in the configuration wizard identify the database principal.

- If you choose **Active Directory Integrated** authentication, the configuration wizard accesses the database as the user running the configuration wizard (an Active Directory user).
- If you choose other authentication modes, then the configuration wizard accesses the database as a different principal.

See Supported authentication types for more information on selecting an admin database principal.

> **Note:**
>
> The database admin principal is only used while running the configuration wizard. It is not saved and not used by the Stream and SOAP services. You must use a principal with elevated privileges for Stream and SOAP services.

- When using SQL Server or Azure SQL Managed Instance, the admin database principal requires the following permissions:
  - `securityadmin` for creating and updating server logins (when using SQL Server or Azure SQL Managed Instance)
  - `db_owner` for any existing database

  To create a database for a new farm, the admin database principal requires `dbcreator` as an additional permission.

- When using Azure SQL Database, the admin database principal requires the following permissions:
  - `loginmanager` for creating and updating server logins (when using Azure SQL Database)
  - `db_owner` for any existing database

  To create a database for a new farm, the admin database principal requires `dbmanager` as an additional permission.

  `loginmanager` and `dbmanager` are special user roles that are assigned to users in the master database.

Service account permissions

The service account for the Stream and SOAP services must have the following system privileges:

- Run as service
- Registry read access
- Access to `Program Files\Citrix\Citrix Provisioning`
- Read and write access to any virtual disk location.

The **service database principal** is the database principal used by the services to access the provisioning database. The authentication credentials you specify in the configuration wizard identify the database principal to be used.

- If you choose **Active Directory Integrated** authentication, the services access the database as the service account (an Active Directory user).
- If you choose other authentication modes, then the services access the database as a different principal.

See Supported authentication types for more information on selecting a service database principal.

The configuration wizard will configure the database to ensure the service database principal has the following permissions.

- `db_datareader`
- `db_datawriter`
- Run permissions on stored procedures

Enable a feature flag on your Azure subscriptions

Enable the `ReserveMacOnCreateNic` feature flag using the following PowerShell commands:

```
Register-AzProviderFeature -FeatureName ReserveMacOnCreateNic
-ProviderNamespace Microsoft.Network

Register-AzResourceProvider -ProviderNamespace Microsoft.Network
```

This PowerShell command only changes the timing when MAC addresses are allocated for virtual NICs and does not change the functionality any other way.

If you want to permanently remove the capability to create target VMs on Azure, you can disable the feature flag as follows:

```
Unregister-AzProviderFeature -FeatureName ReserveMacOnCreateNic
-ProviderNamespace Microsoft.Network
```

Create one or more Resource groups on Azure

Using the Azure documentation, create the Resource groups that match your required structure.

Set up Active Directory

Use one of the following methods to support Active Directory APIs and functionality on Azure:

- Enable Azure Active Directory Domain Services feature for the Azure tenant (directory). If you require connectivity with your corporate Active Directory service, install and configure Azure AD Connect on a server in your data center. Azure AD Connect provides synchronization between your on-premises domain controllers and the Azure AD directory. This process can be integrating with your on-premises forest using the Microsoft AD Connect feature.
- Create Active Directory domain controller VMs in your subscription and connect to an on-premises forest via an ExpressRoute connection.
- Create a stand-alone Active Directory domain by creating AD Domain Controllers in your subscription.

Citrix Provisioning on Azure also supports Hybrid Azure AD. Set up Hybrid Azure AD and enable Microsoft Entra Connect Sync on the Domain Controller. For information, see Configure Microsoft Entra hybrid join. For information on creating a Hybrid Azure AD catalog, see Create Hybrid Azure AD joined catalogs.

Establish a virtual network for streaming on Azure

If you do not already have a virtual network on Azure, create a virtual network per region and subscription that you are using. There must be virtual network peering to the Active Directory virtual network and to the Azure SQL Managed Instance virtual network (if used). Refer to the Azure instructions, Establish a Virtual Network.

1. Set up virtual network peering between the virtual network that is set up to stream targets, and the virtual network running Active Directory. These peerings allow connected VMs to communicate with the Domain Controllers for your Active Directory domain. Citrix recommends using a standard *Hub and Spoke* configuration for your virtual networks. See Hub-spoke network topology in Azure.
2. Set the DNS servers for each virtual network to the AD Domain Controllers' IP addresses.

(Recommended) Set up Azure Bastion access for secure VM access

For secure external access to VMs running in the subscriptions, we strongly recommend that you create your infrastructure VMs with NO public IP address and configure Azure Bastion, as described in the Azure documentation, Configure Bastion.

Create a connector VM on Azure

Create VMs to act as cloud connectors in each unique combination of region and subscription you are using. Then, install a Citrix Cloud Connector.

Create the Citrix Provisioning Server on Azure

On Azure, create VMs for the provisioning servers. Size servers for the expected load, similar to on-premises provisioning servers. Then install the Citrix Provisioning software on the VMs.

Configure hosting connection for US Government

Citrix Provisioning supports Azure control planes other than Azure Commercial, including Azure for US Government. You can add the management URL `<https://management.usgovcloudapi.net/>` for the Azure US Government while creating the hosting connection using Citrix Studio. For information, see Create a connection using an existing service principal.

Configure service endpoint URLs

Azure has a secret environment where the endpoints of Azure services are a secret. To support the Azure secret region, you can now configure endpoint URLs of required services.

To configure endpoint URLs:

1. Ensure that the path `C:\ProgramData\Citrix\Citrix Provisioning\Config` exists on all the Citrix Provisioning Servers.
2. Set Access Control List (ACLs) on the `Config` folder to protect the `config` JSON file from unauthorized access. The recommended ACLs are as follows:
   - System: Full Control. This permission applies to folders, subfolders, and files.
   - Administrators: Full Control. This permission applies to folders, subfolders, and files.
   - Any specific user to run Citrix Provisioning services: Read Only. This permission applies to folders, subfolders, and files. If you do not specify the permission, Citrix Provisioning services run as Network Service. In this case, you must grant Read permission to Network Service.
3. Create a JSON file `CustomizedAzureEnvironmentConfig.json` under the `Config` folder. Enter the endpoint URLs in the JSON file. For example:

   ```
   {

   "managementEndpoint": "https://management.scombine.scloud/",

   "databaseEndpoint": "https://database.scombine.scloud",

   "loginEndpoint": "https://login.scombine.scloud/",

   "graphEndpoint": "https://graph.scombine.scloud/",

   "storageSuffix": ".scombine.scloud"

   }
   ```

4. Enable the feature flag.
   a. Add a DWORD value `AzureSecretRegion` in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices\Features`.
   b. Set the value to `1`.

Install the Citrix Provisioning software

The Citrix Provisioning Server VMs require the following resources:

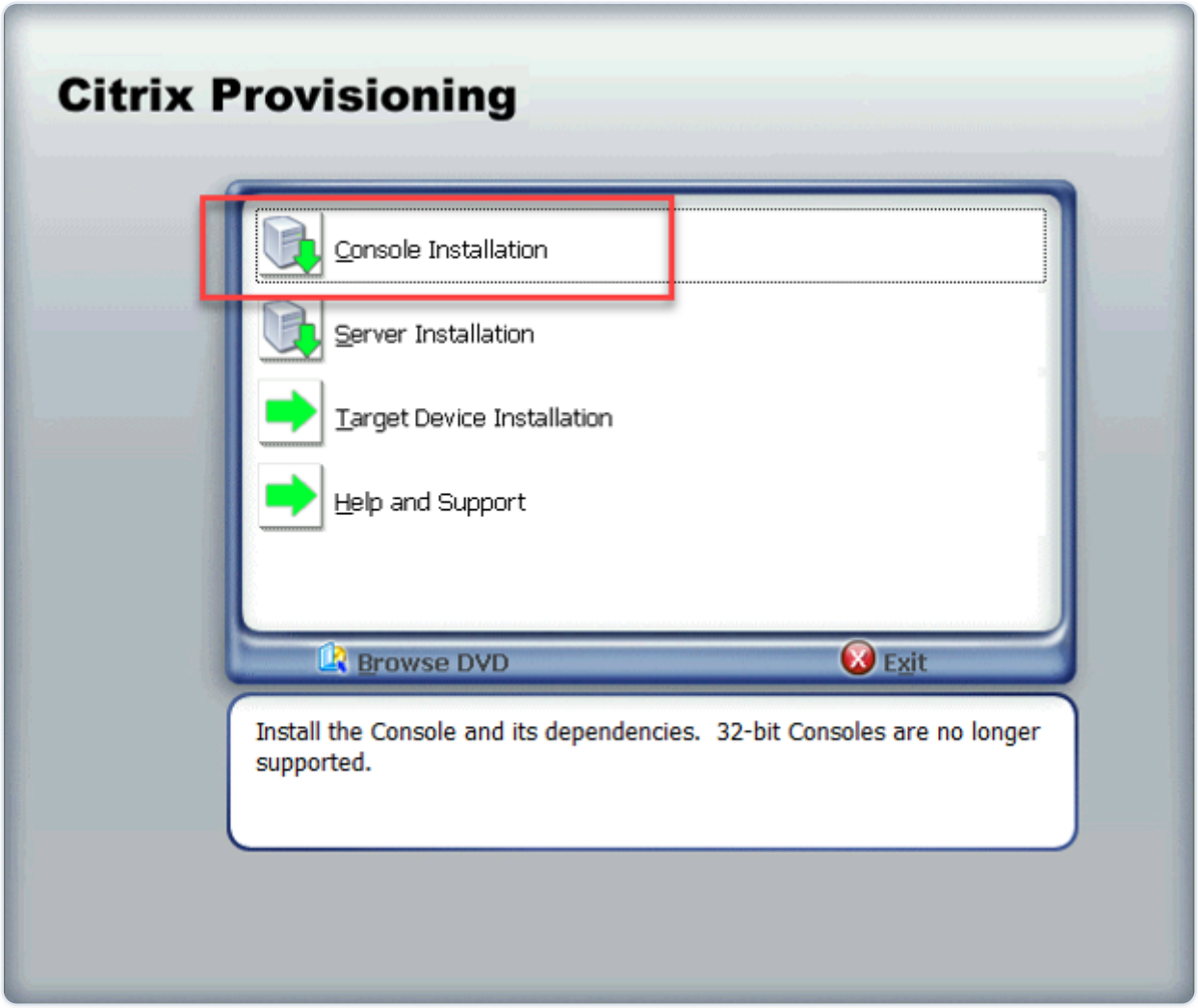
- Access to an Azure SQL Database service or Azure SQL Managed Instance service, or a VM running SQL/Server or SQL/Server Express.
- Access to a license server VM on Azure.
- The Active Directory requirements are the same as for the existing on-premises version of Citrix Provisioning.
- A suitable virtual network and subnets to support the traffic. We strongly recommend NO public IP addresses, and access only using the Bastion Service. If you have multiple virtual networks, configure peering to one or more subnets containing the provisioning server, the licensing server, and Active Directory. If you have multiple virtual networks and subnets, Citrix recommends setting up a standard *Hub and Spoke*. See Hub-spoke network topology in Azure.
- For streaming, Citrix Provisioning servers require a minimum of one Network Interface Card (NIC) that target devices can use for communication.
- Access to virtual disk storage. You can use:
  - Local storage on the Provisioning Server VM (typically via an Azure Data Disk).
  - On a file share implemented by a Premium Azure Storage Account, or Azure Netapp Services.

    > **Reminder:**
    >
    > If you use a file share, reference it by UNC in the Citrix Provisioning setup. For example, \\server01\path\path.
    >
    > Citrix Provisioning does not support Standard Storage Accounts. If you use an Azure File Share, follow the instructions to provide access for the StreamServer to the file share in Azure.

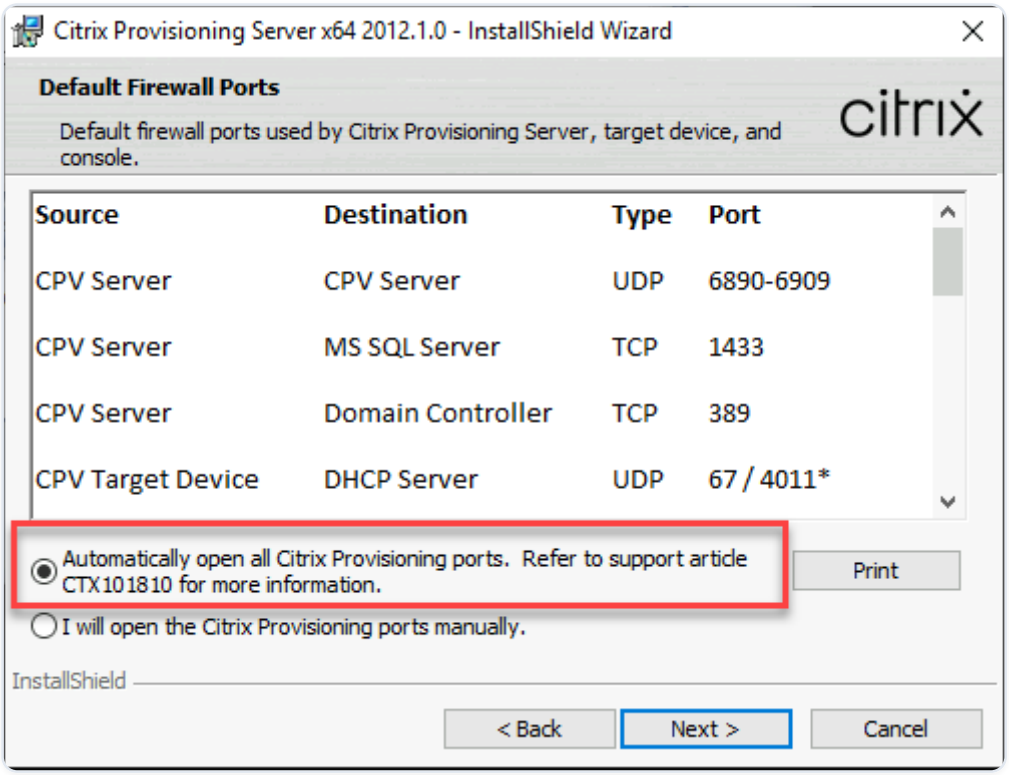
  - On a separate VM providing a file share.
- Minimum of two 4vCPUs, 8 GB RAM each for the Citrix Provisioning Server VM. The more GBs, the better. Two 4vCPU with 16 GB Citrix Provisioning Servers with accelerated networking enabled are enough to handle 2500 targets streaming one vDisk.

To install the Citrix Provisioning Server and Console:

1. Using an administrator account, log into the Citrix Provisioning Server VM (through the Bastion Host, if using Bastion).
2. In File Explorer, select the ISO file, right click, and mount it.
3. In the mounted drive's root folder, find the **autorun.exe** file, and run it. The Citrix Provisioning Installer starts.
4. Start by installing the Console. The installer prompts you to install prerequisites.



5. If prompted, reboot, mount the Citrix Provisioning ISO again, and restart the process.
6. Install the Citrix Provisioning Server using the **Server Installation** link on the autorun program. By default, creating firewall rules for provisioning traffic is enabled.



Note:

Ensure any Network Security Group defined for the VNets must allow Citrix Provisioning traffic to flow. See Communication Ports Used by Citrix Technologies for information on ports that must be opened to ensure communication flow.

When the server installation completes, it runs the Citrix Provisioning Configuration Wizard where you set up the provisioning server.

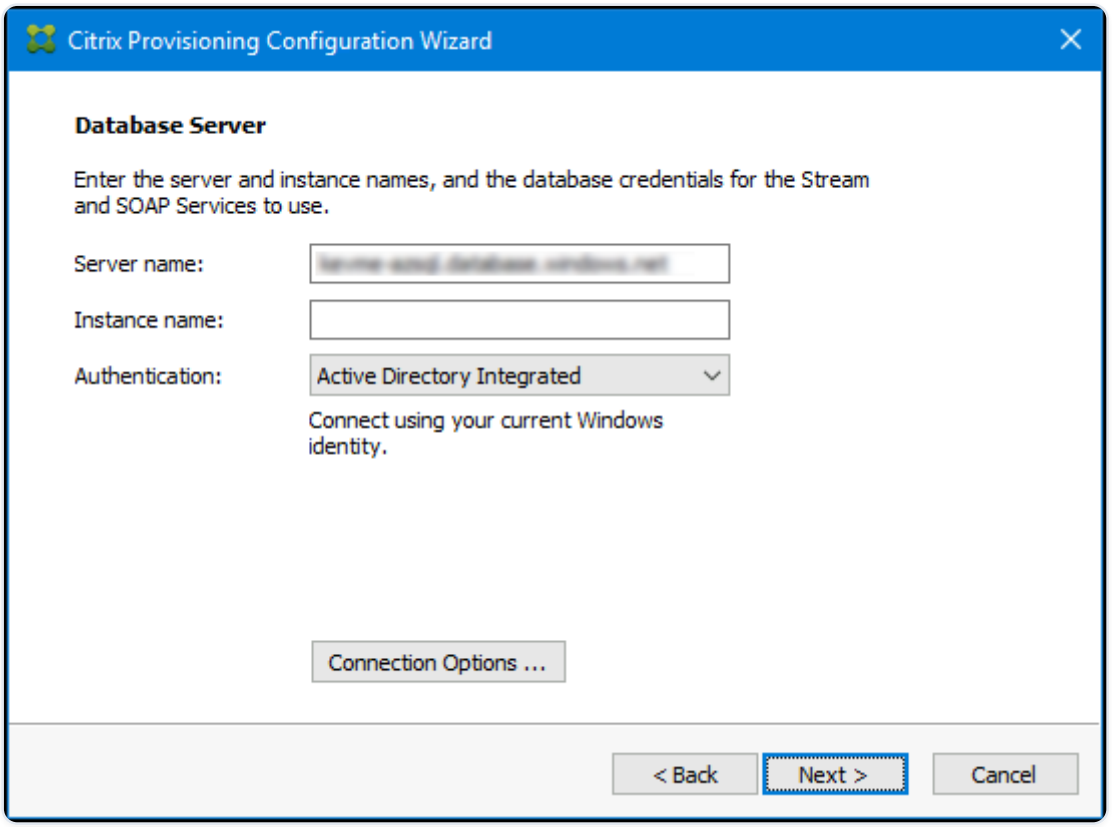
a. Welcome: Read the Welcome dialog and click **Next**.

b. Farm configuration: Indicate you want to create a new farm.

   If you select **Farm is already configured**, enter database administrator credentials in the pop-up dialog. Select **Active Directory Integrated** authentication if you want to use the current login.

c. Database Server: Enter the SQL Server host name or address and the name of the instance you created for the provisioning server to use, or add the Azure SQL Database server name (leave instance blank), or the Azure SQL Managed Instance host name (leave instance blank). The Authentication drop-down lists the supported authentication types. Depending on the authentication mode that is selected, you can provide the necessary

credentials to connect to the database. The credentials on this page are for the Stream and SOAP services.



After you click Next, enter database administrator credentials in the pop-up dialog. Select **Active Directory Integrated** authentication if you want to use the current login.

d. New Farm: Enter the farm, site, and collection names. We recommend selecting Use Active Directory groups for security, and the Farm Administrator group.

e. New Store: Specify the store and location. If you are using a file share, then enter a UNC name.

f. License Server: Enter the license server location.

g. User Account: Specify the user account to run the services under. If you use a network share for the store, use a domain account with access to the share. The account must be an administrator on the PVS server.

h. Network Communication: Choose the network interface to be used for streaming and management. If you only have a single NIC, accept the defaults.

i. Soap SSL Configuration: Accept the default values.

j. Problem Report Configuration: Enter your MyCitrix credentials to enable submission of cases.

k. Finish: Review the configuration settings, and click **Finish**. A dialog reports a warning about the Windows Firewall.

l. Click **OK**. A progress dialog opens to display progress as Citrix Provisioning is being configured. If failures occur, you receive a link to review the log.

m. When configuration is successful, click **Done**.

Workflow for running the configuration wizard silently

The basic steps involved in the silent configuration of servers in the farm are:

- Create a `ConfigWizard.ans` file from a configured provisioning server in the farm, or create the file manually. To create the file manually, see Create the ConfigWizard.ans file manually.
- Copy the `ConfigWizard.ans` file onto the other servers in the farm, and modify the IP address in the `ConfigWizard.ans` file to match each server in the farm.
- Run `ConfigWizard.exe` with the `/a` parameter.

Create the ConfigWizard.ans file manually

If you want to create the `ConfigWizard.ans` file from scratch, using a text editor that lets you save as Unicode, create a file named `ConfigWizard.ans`, and save it as Unicode. Enter the parameters shown in the table. Include all of the parameters relevant to your configuration.

SCREEN	UI OPTION	MANUAL PARAMETER
Farm Configuration	**Farm is already configured**	FarmConfiguration=0
	Create farm	FarmConfiguration=1
	Join existing farm	FarmConfiguration=2
Database Server	**DatabaseAdminAuthentication**	DatabaseAdminAuthentication=`<` *ActiveDirectoryIntegrated*, *ActiveDirectoryPassword*, or *SqlPassword* `>`
	DatabaseAdminUsername	DatabaseAdminUsername=`<` *Active Directory username* or *SQL login* `>` (Used only if DatabaseAdminAuthentication is ActiveDirectoryPassword or SqlPassword)

SCREEN	UI OPTION	MANUAL PARAMETER
	DatabaseAdminPassword	DatabaseAdminPassword=< *password* > (Used only if DatabaseAdminAuthentication is ActiveDirectoryPassword or SqlPassword)
Database Server (after **Create Farm** or **Join existing farm**)	**DatabaseAuthentication**	DatabaseAuthentication=< *ActiveDirectoryIntegrated*, *ActiveDirectoryPassword*, *ActiveDirectoryServicePrincipal*, *ActiveDirectoryMSI/System*, *ActiveDirectoryMSI/User*, or *SqlPassword* >
	DatabaseUsername	DatabaseUsername=< *Active Directory username*, *App Registration name*, *Managed Identity name*, or *SQL Login* > (Used only if DatabaseAuthentication is ActiveDirectoryPassword, ActiveDirectoryServicePrincipal, ActiveDirectoryMSI/User or SqlPassword)
	DatabasePassword	DatabaseAdminPassword=< *password* or *application secret* > (Used only if DatabaseAuthentication is ActiveDirectoryPassword, ActiveDirectoryServicePrincipal, or SqlPassword)
	DatabaseTenantID	DatabaseTenantID= < Tenant ID of application registration > (Only used if DatabaseAuthentication is ActiveDirectoryServicePrincipal)

SCREEN	UI OPTION	MANUAL PARAMETER
	DatabaseApplicationID	DatabaseApplicationID= < Application ID of application registration > (Only used if DatabaseAuthentication is ActiveDirectoryServicePrincipal)
	DatabaseClientID	DatabaseClientD= < Client ID of Managed Identity > (Only used if DatabaseAuthentication is ActiveDirectoryMSI/User)
	DatabaseObjectID	DatabaseObjectID= < Object ID of Managed Identity > (Only used if DatabaseAuthentication is ActiveDirectoryMSI/User)
	Server name	DatabaseServer=`<` *dBName* `>`, `<` *NonDefaultSQLPort* `>` (If default port, omit port value)
	Instance name	DatabaseInstance=`<` *InstanceName* `>`
	Database name	DatabaseNew=`<` *DbName* `>`
	Enable MultiSubnetFailover for SQL Server Always On	MultiSubnetFailover=`<` *0 or 1* `>`
	Database Mirror Failover Partner Server Name	FailoverDatabaseServer=`<` *dBName* `>`, `<` NonDefaultSQLPort `>` (If a database mirror failover partner is not used, this value is omitted, or has an empty value)

SCREEN	UI OPTION	MANUAL PARAMETER
	Database Mirror Failover Partner Instance Name	FailoverDatabaseInstance=`<` *InstanceName* `>` (If a database mirror failover partner is not used, this value is omitted, or has an empty value)
New Farm (when new farm is created)	**Farm name**	FarmNew=`<` *FarmName* `>`
	Site name	SiteNew=`<` *SiteName* `>`
	Collection name	CollectionNew=`<` *CollectionName* `>`
	Farm Administrator group: PVS server is in Active Directory	ADGroup=`<` *Path to AD group* `>` Ex: `test.local/Users/Domain Users`
	PVS server is in Workgroup	Group=`<` *Path to local group* `>` Ex: PVS-Server-1/Administrators
New Store (when new farm is created)	**Store name**	Store=`<` *StoreName* `>`
	Default path	DefaultPath=`<` *Store path* `>`
Existing Farm (when joining an existing farm)	**Farm name**	FarmExisting=`<` *database name* `>`
Site (when joining an existing farm)	**Existing site; Site name**	ExistingSite=`<` *Site name* `>`
	New site; Site name	Site=`<` *Site name* `>`
	Collection name	Collection=`<` *Collection name* `>`
Store (when joining an existing farm)	**Existing store; Store name**	ExistingStore=`<` *Store name* `>`

SCREEN	UI OPTION	MANUAL PARAMETER
	New store; Store name	Store=<*Store name*>
	Default path	DefaultPath=<*Path to store*>
License Server	**License server name**	LicenseServer=<*Citrix License Server's IP, host name, FQDN*>
	License server port	LicenseServerPort=<*LicenseServerPort*> (27000 is default port)
	On-premises (license type)	licenseSKU=0
	Use Datacenter licenses for desktops if no Desktop licenses are available	LicenseTradeup=<*0 or 1*>
	Cloud (license type)	licenseSKU=1
User account	**Network service account**	Network=1
	Specified user account; User name/Domain	<*domain\username*>
	Password	UserName2=<*Password*>
Active Directory Computer Account Password	Days between password updates	PasswordManagementInterval=<*#ofDays*> (Including this parameter enables **Automate computer account password updates**)
Network Communications	**Streaming network cards**	StreamNetworkAdapterIP=<*IPofStreamingNIC1,IPofStreamingNIC2,...*> (comma-separated list of IPs)

SCREEN	UI OPTION	MANUAL PARAMETER
	Management network card	ManagementNetworkAdapter IP=<*IPofManagementNIC*> (only one IP)
	Note: Network cards can be both streaming and management.	
	First communications port	IpcPortBase=6890
	Total ports used for server communication	IpcPortCount=20
	Console port	SoapPort=54321
Soap SSL Configuration	**SSL port**	SSLPort=54323
	SSL certificate	SSLCert=<*token*>
Problem Report Configuration	**My Citrix Username**	CisUserName=<*username*>
	Password	CisPassword=<*password*>

Create the master VM

This section explains how to create the master VM, and preparing the image to connect to the Citrix Provisioning Server at boot time.

Be sure to use:

- A Generation 2 machine.
- Windows 10, Windows 11 (Standard Security Type), or Windows Server 2016/2019/2022 OS.

To create the master VM:

1. Create a Virtual Machine:

    a. Log on to the Azure Portal, and go to **Home > Virtual Machines**.

    b. Click **Add**, and complete the **Create Virtual Machine** wizard. Be sure to set these values:

- Basics: At the bottom of the page, select the **I confirm** Licensing option.
- Networking: Specify the subnet used for streaming, and choose **no public IP**.
- Advanced: Ensure VM generation **Gen 2** is selected.

c. Complete the Windows Setup.

d. Join the domain used by your Citrix Provisioning deployments.

e. Deploy the VDA, using standard practices.

2. Ensure that the pagefile location is correct.

   - If the machine size chosen has a temporary disk, ensure that the system pagefile is located on this disk (drive letter D:). If you created the master VM from an Azure Marketplace image, the system pagefile must already be located on the temporary disk. However, if the VM was created from your own image, this might not be the case.
   - If the machine size does not have a temporary disk. The system pagefile must be located on the boot (C:) disk.

3. Install the Citrix Provisioning Target Device software.

   a. Mount the Citrix Provisioning ISO.

   b. Reboot when prompted.

4. Run the imaging wizard or P2PVS, as you would for an on-premises installation.

   a. Specify the **Server name or IP address**, and select **Use my Windows credentials**.

   b. Imaging Options: Select **Create a vDisk**.

   c. Add Target Device: Specify the **Target device name** and the **Collection name**.

> **Important:**
>
> Use a different name than the current host name. The master VM can boot either from the local disk or from the virtual disk you create, but Computer Account password management is not synchronized between them. If you give the target the same name as the current host, you lose domain trust when switching between the two ways of booting the master VM.

   d. New vDisk: Specify the virtual disk name.

e. Microsoft Volume Licensing: Select **KMS Licensing**.

f. What to Image: Select **Image entire boot disk**.

g. Optimize Hard Disk for Citrix Provisioning: Select **Optimize the hard disk** to ensure that unnecessary Windows features are disabled.

h. Summary: Verify that the settings are correct, and click **Create** when prompted, reboot the VM. As the VM reboots, the Azure Boot Diagnostic page in the Azure portal displays the boot progress.

i. When the Master VM finishes booting, log on again. The imaging wizard resumes where it left off. A dialog asks whether to format the disk. Select **Cancel**. (The imaging takes some time.)

j. When imaging is complete, exit the imaging wizard.

k. On the provisioning console:

- Update the vDisk to Production status, with **Cache Type** set to **Cache in device RAM with overflow on hard disk**.
- Right-click the master VM target definition, and select **Active Directory > Create Computer Account**.

Create target VMs on Azure using the Citrix Virtual Apps and Desktops Setup Wizard

The Citrix Virtual Apps and Desktops Setup Wizard lets you create multiple target VMs in a single invocation. The wizard guides you through the complete process of creating target VMs and integrating them with Citrix Virtual Apps and Desktops and Citrix DaaS.

Initial Setup

Do the following once before running the Citrix Virtual Apps and Desktops Setup wizard:

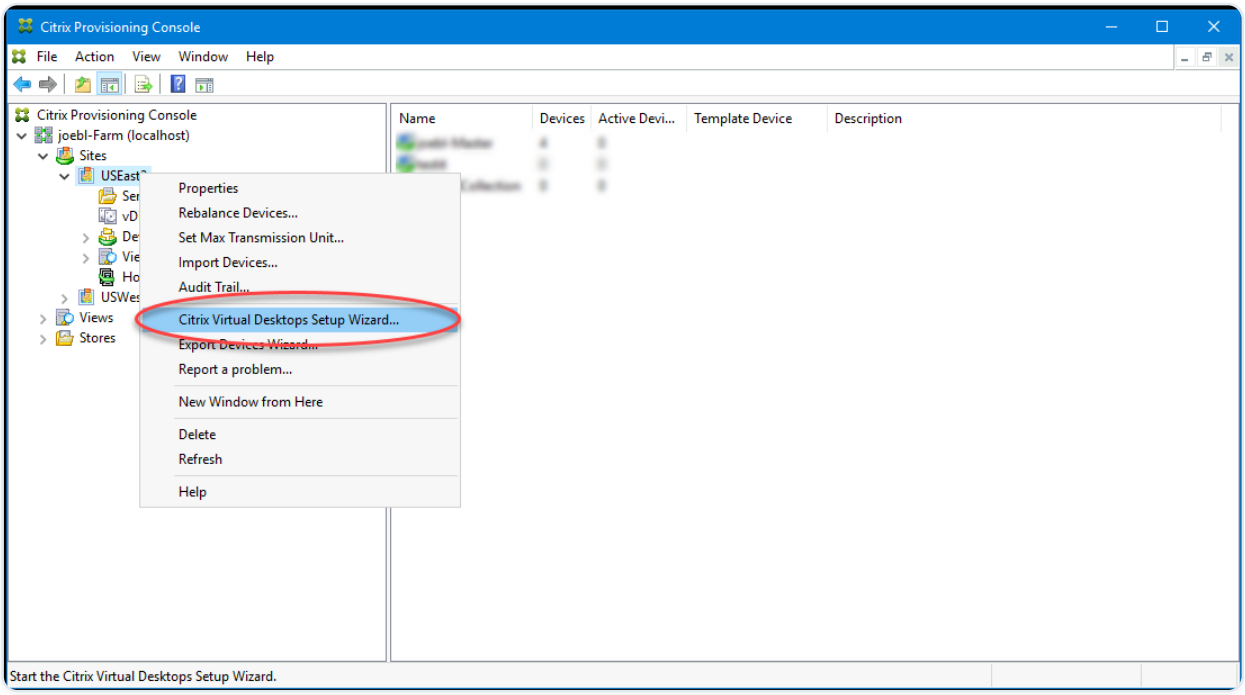
1. If you want to use your own Service Principal for accessing Azure, follow the guidance in Microsoft Azure Resource Manager virtualization environments to create an SPN suitable for use with provisioning.

> **Note:**
>
> Do not use **CanNotDelete** or **ReadOnly** locks on resource groups that are used in the Citrix Virtual Apps and Desktops Setup wizard. See Microsoft Lock Resources for details.

Create target VMs

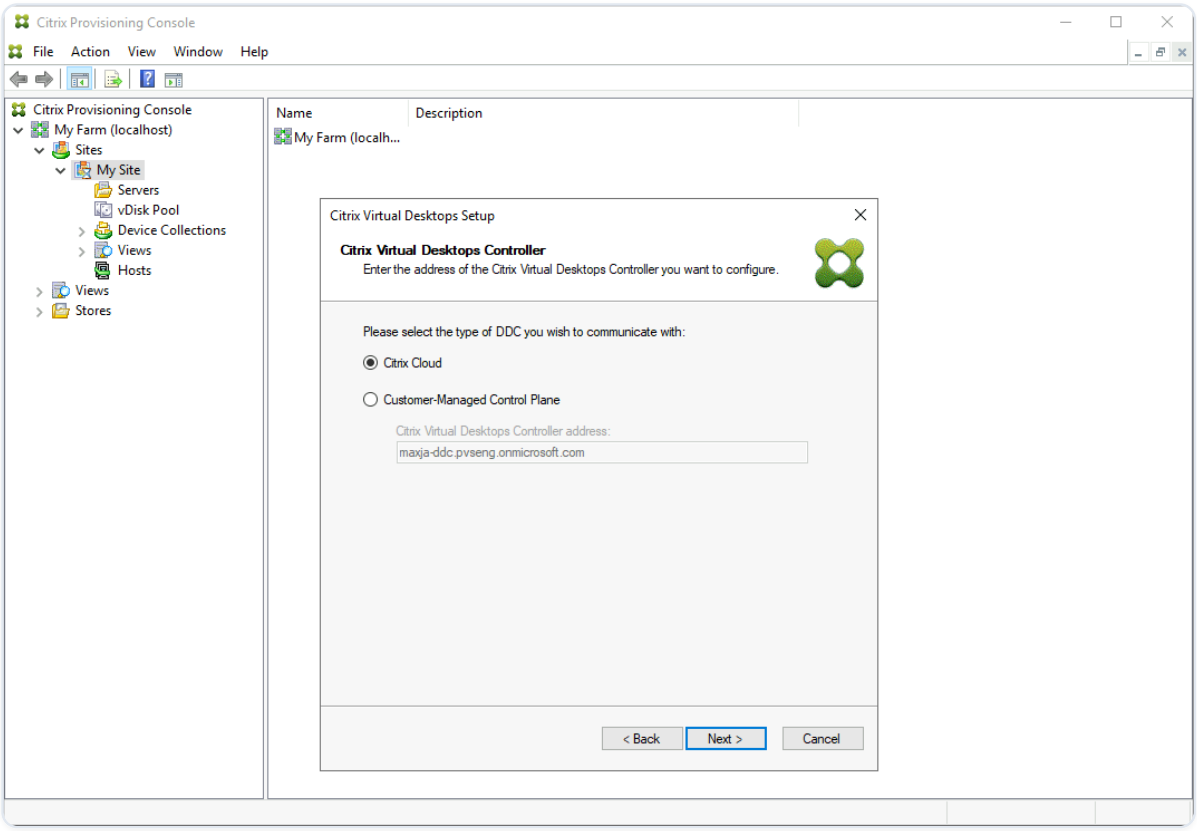
To create target VMs using the wizard:

1. Run the provisioning console, right-click the site where you want to create targets, and select **Citrix Virtual Desktops Setup Wizard**.



2. Click through the welcome page, select the type of Delivery Controller, and choose **Next**.

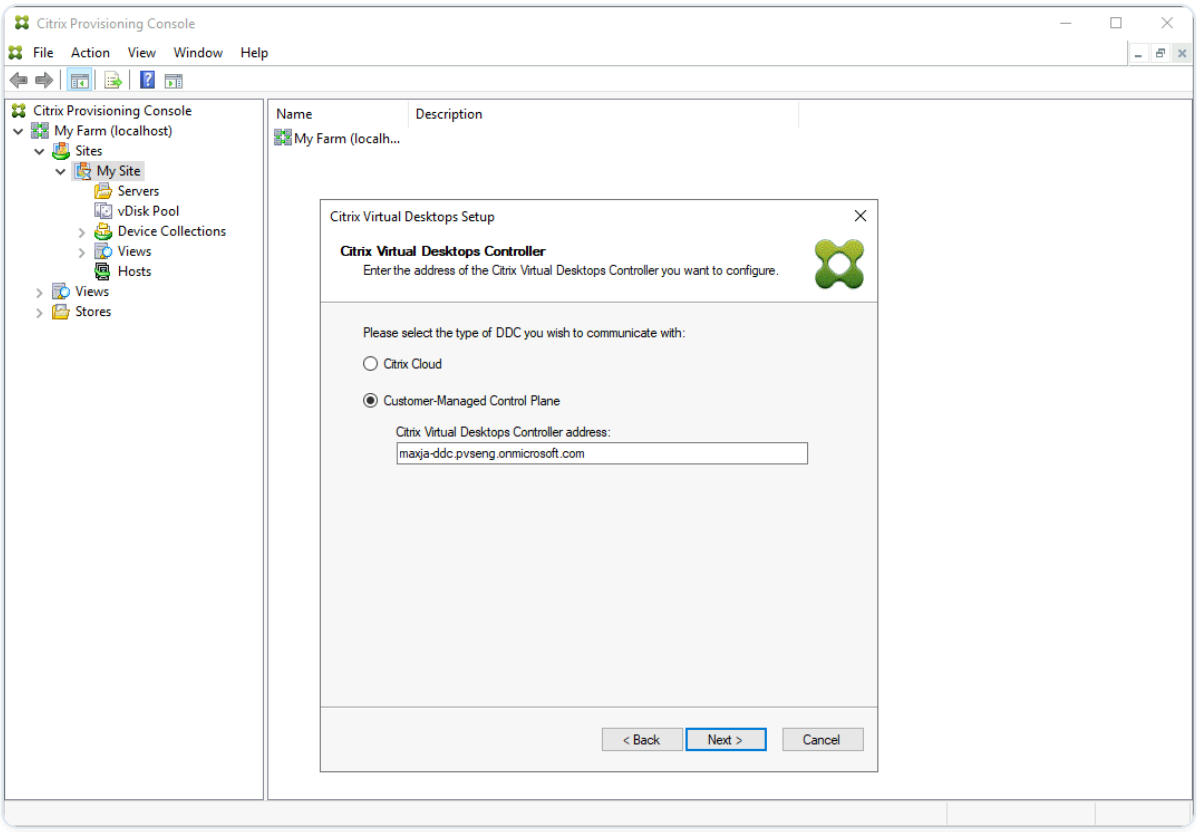
    a. If you select **Citrix Cloud**:



i. Enter Citrix Cloud credentials.

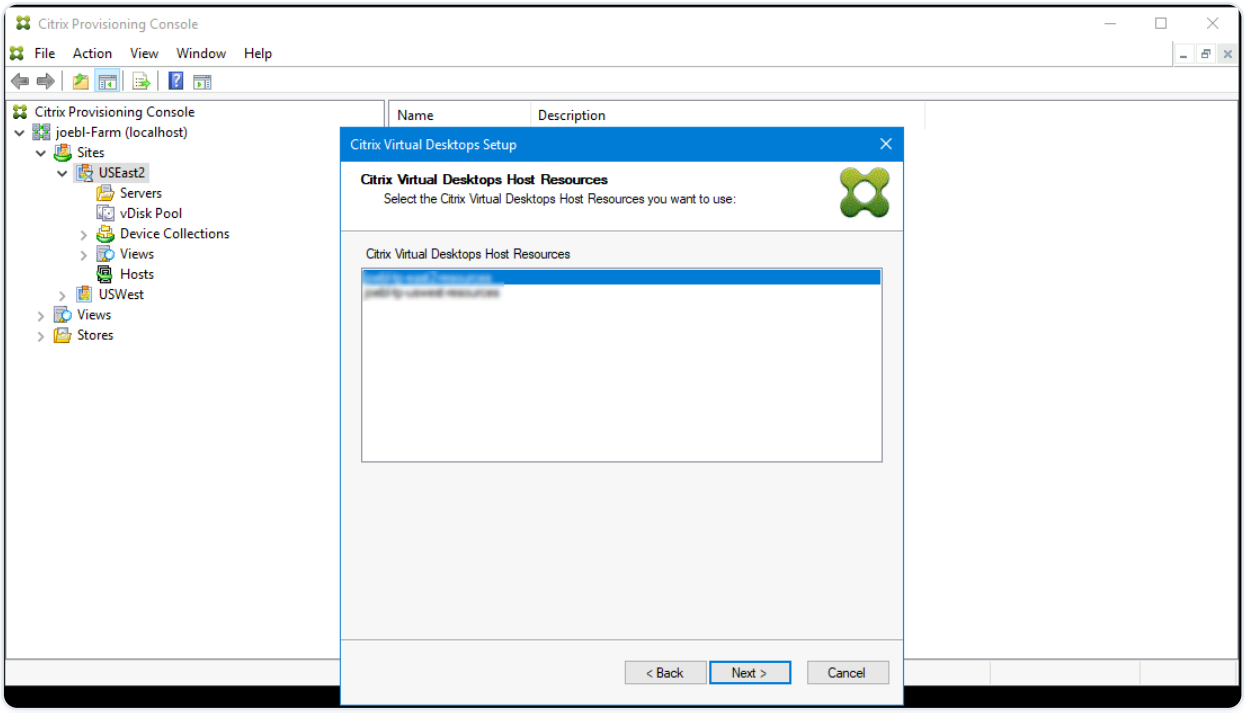
ii. If you have more than one customer, select appropriate cloud customers.

b. If you select **Customer-Managed Control Plane**:



i. Enter the controller hostname or address. The wizard authenticates to the Delivery Controller using the current logged in user.

3. Choose an Azure hosting unit from the displayed list. The wizard displays the list it retrieves them from the Cloud. Select the hosting unit to use based on the resource location you are provisioning to.



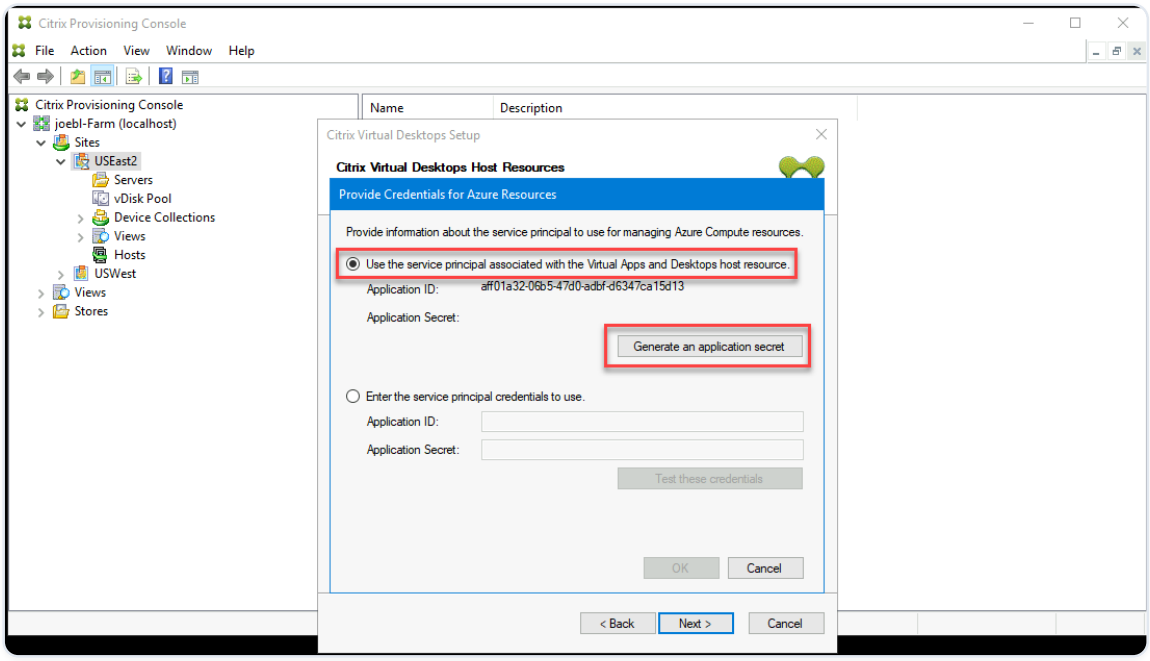
4. Next, establish a Service Principal Name (SPN) for working with the Azure APIs. An SPN has two components:

   - The Application ID, a GUID uniquely identifying the Service Principal.
   - The application secret.

   You have two choices for specifying the SPN:

   - The hosting unit has a configured Application ID. The setup wizard can generate a new secret for this application. However, you need the credentials for the user that initially created the application ID stored in the hosting unit. Continue as follows:

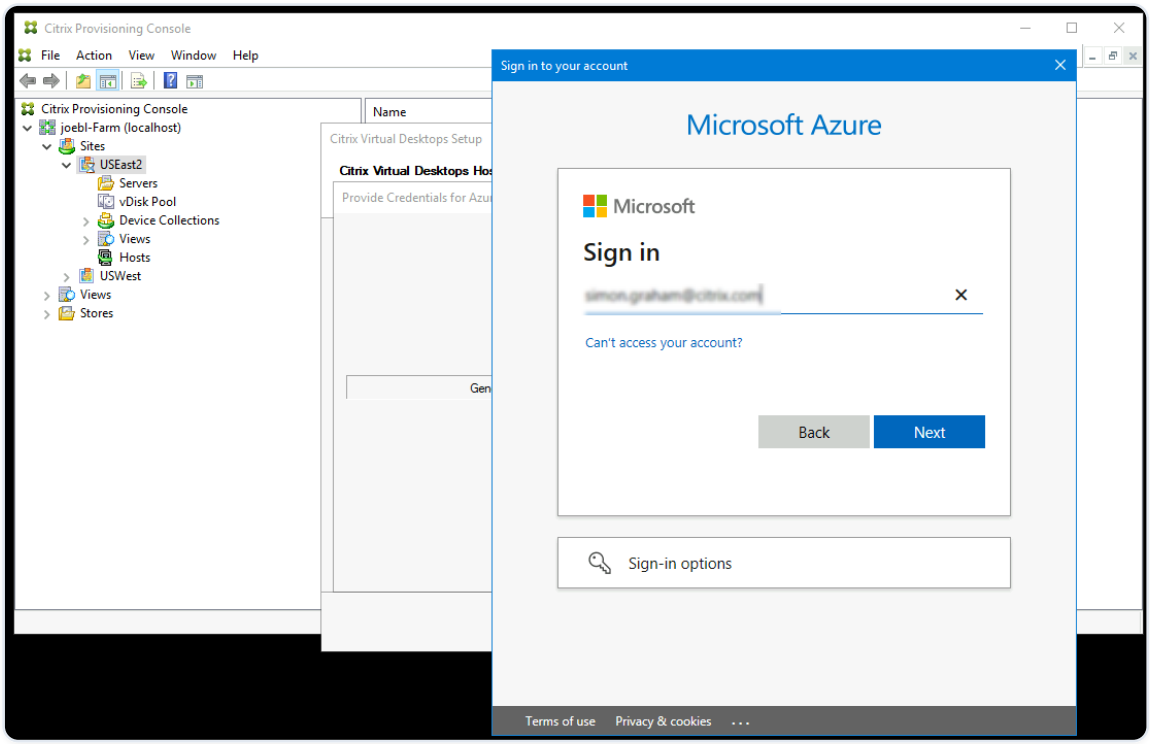
     a. Select **Use the service principal associated with the Virtual Apps and Desktops host resource**, and click **Generate an application secret**.



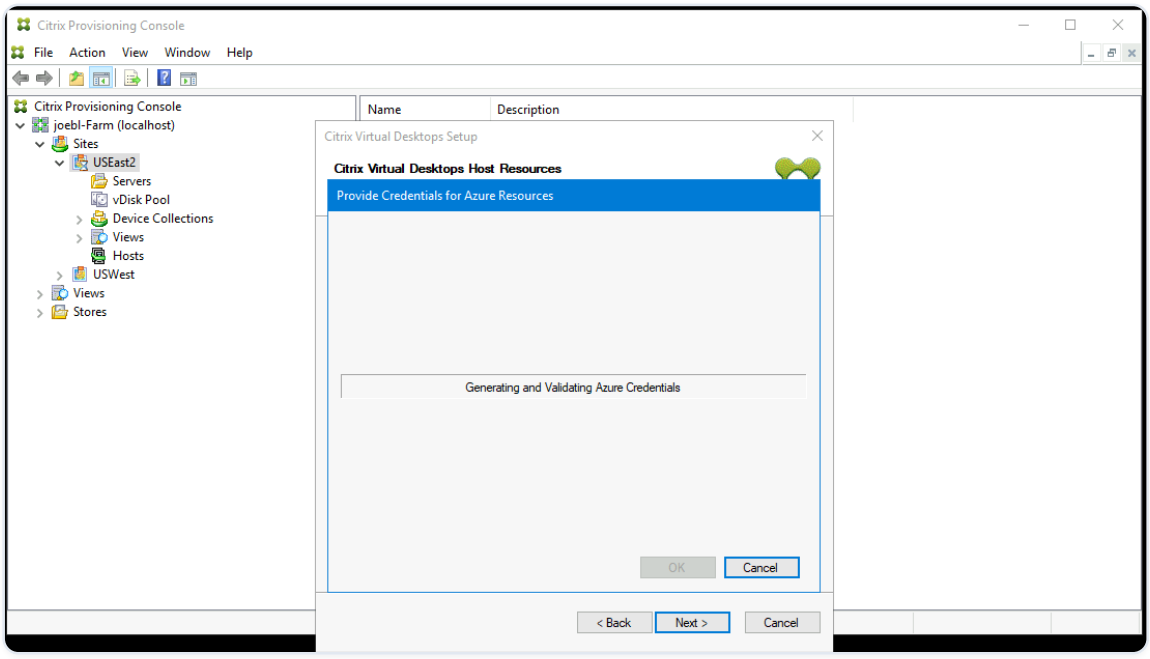
Tip:

When you run the Citrix Virtual Apps and Desktops Setup Wizard for the first time, the selected hosting unit, in this case an Azure hosting unit, the generated secret is valid for one year. The information about the generated secret is displayed. If the generated secret is valid for one year, it is stored in the Citrix Provisioning database and is used for power management operations. When you run the Citrix Virtual Apps and Desktops Setup Wizard again using the same hosting unit, the generated secret is valid for one day. This secret is deleted when you complete the setup process using the setup wizard. If you cancel the setup process while the Citrix Virtual Apps and Desktops Setup Wizard is running, the generated secret is deleted.

b. Sign into Azure using the same credentials used to create the application. If you use different credentials, you get an error.

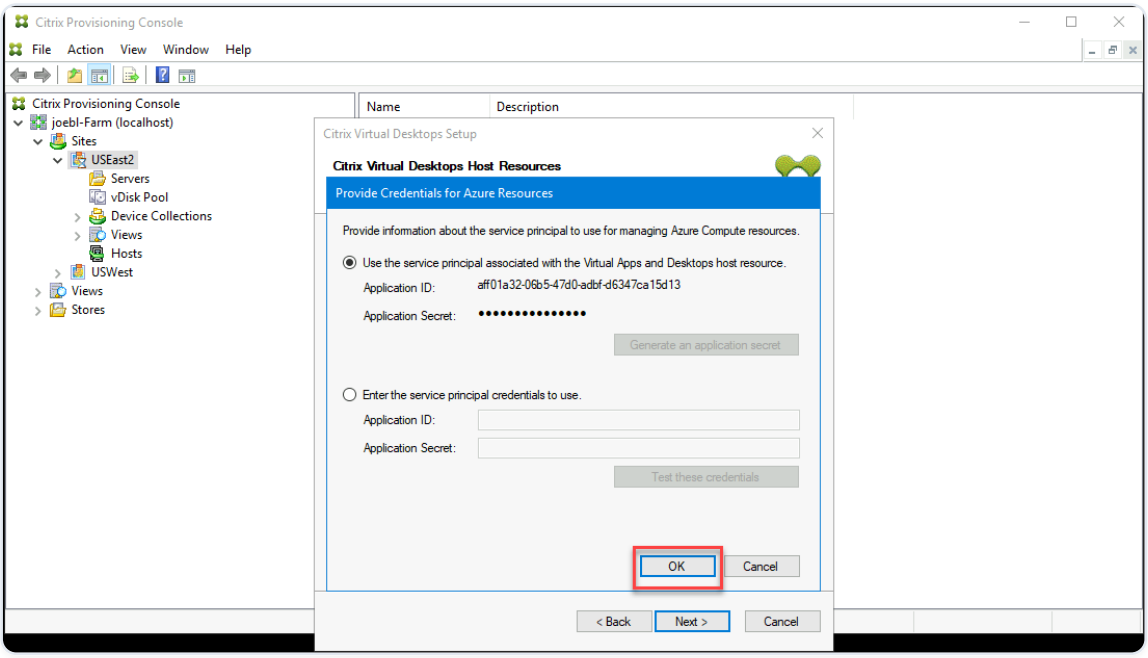


This process can take a significant amount of time. You can press the cancel button to abort if you think it is hung:



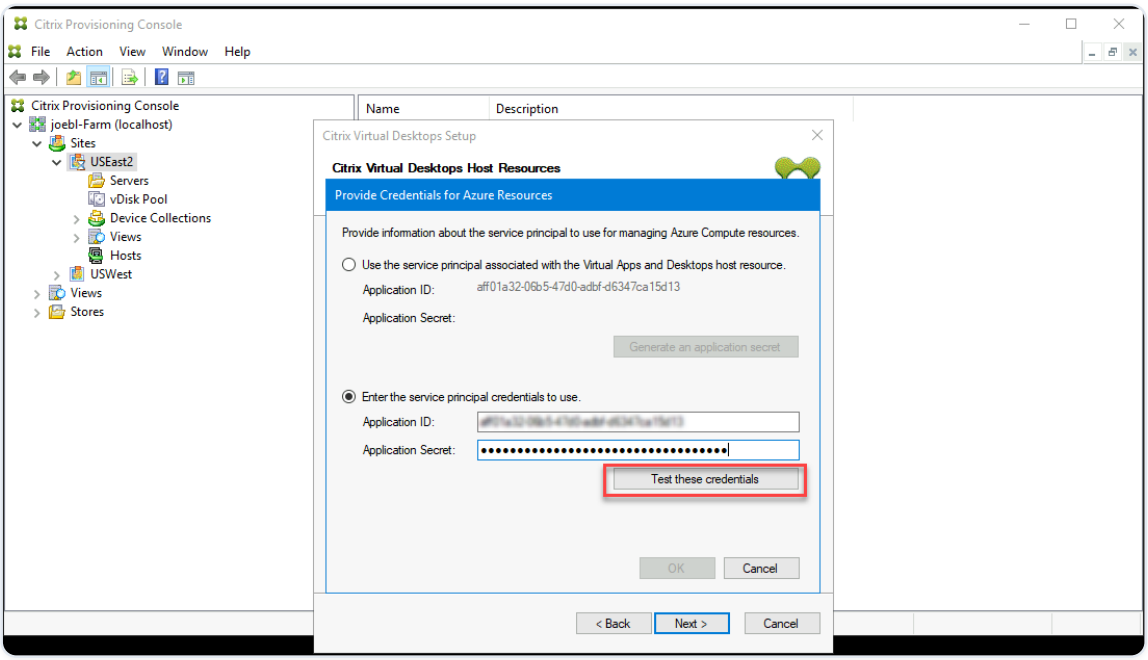
If you cancel, you are taken back to the screen to generate or enter authentication information

c. Once successful, the secret is shown as a set of asterisks. Click **OK** to continue.



- If you previously created your own SPN:

  a. Select **Enter the service principal credentials to use**, and enter your application ID and secret. Click **Test these credentials**.



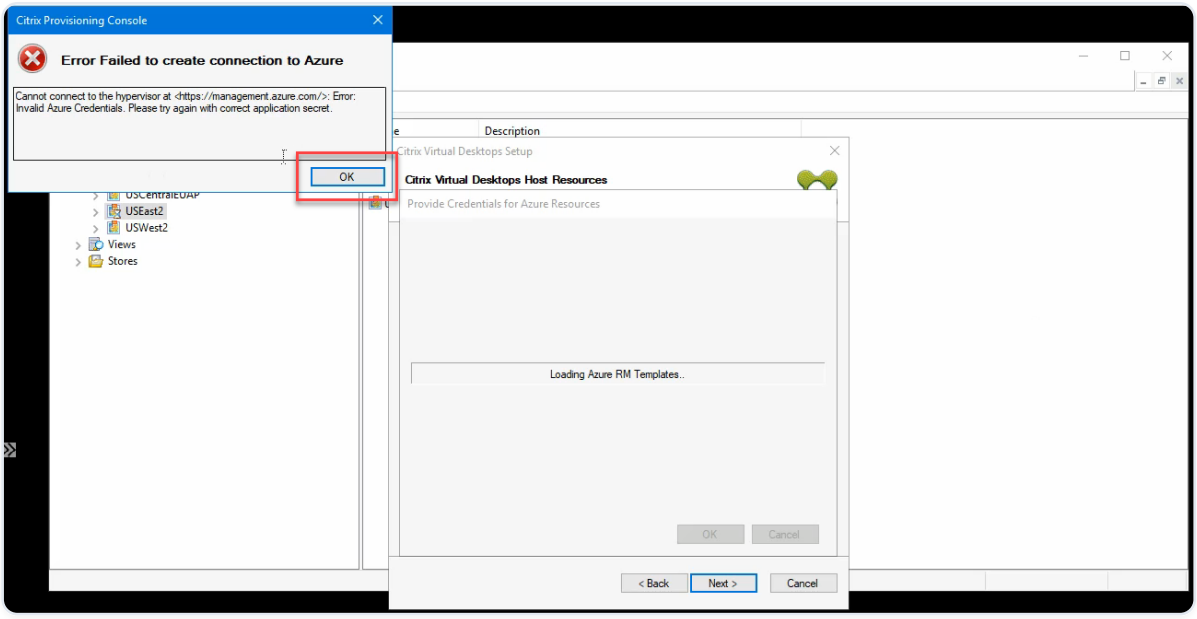
  If the SPN is valid, a green check mark is displayed beside the **Test** button.

  b. Click **OK** to continue. The wizard loads a list of VMs that you can use as the template for creating target VMs.

> **Reminder:**

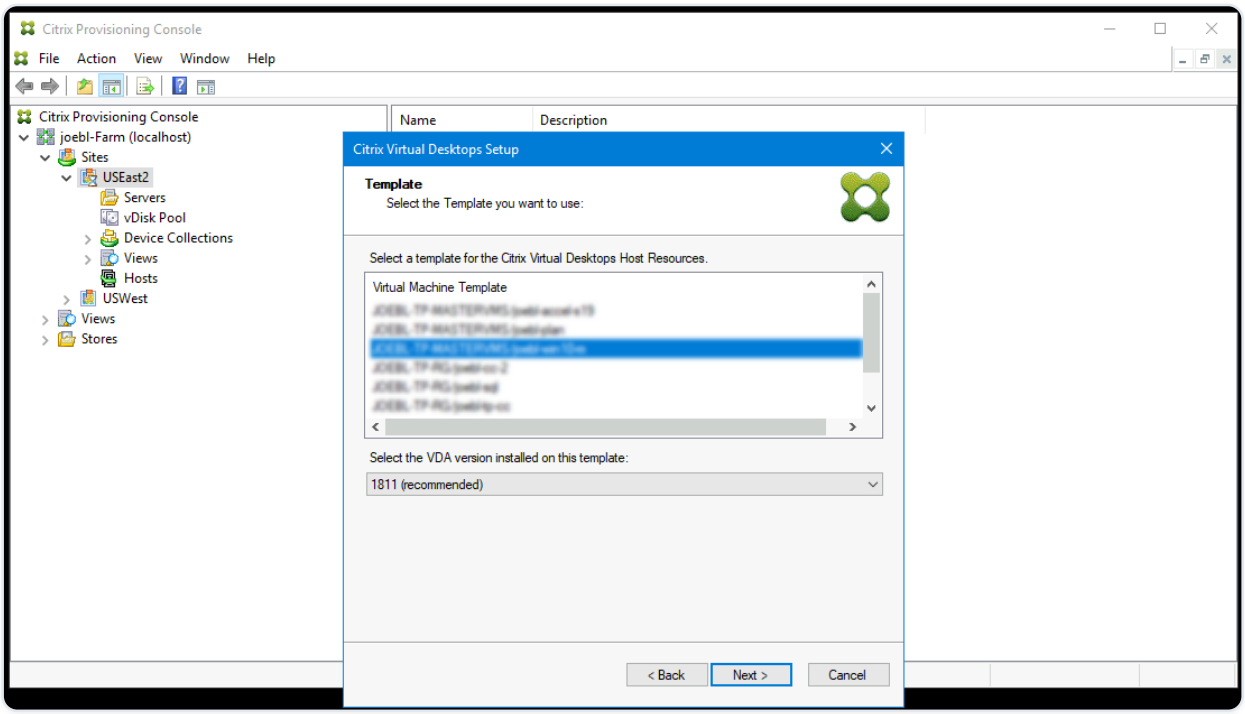
> When you run the Citrix Virtual Apps and Desktops Setup Wizard for the first time using an Azure hosting unit, the credentials are stored in the Citrix Provisioning database for power management operations.

> If the process fails, a message similar to this one is displayed:



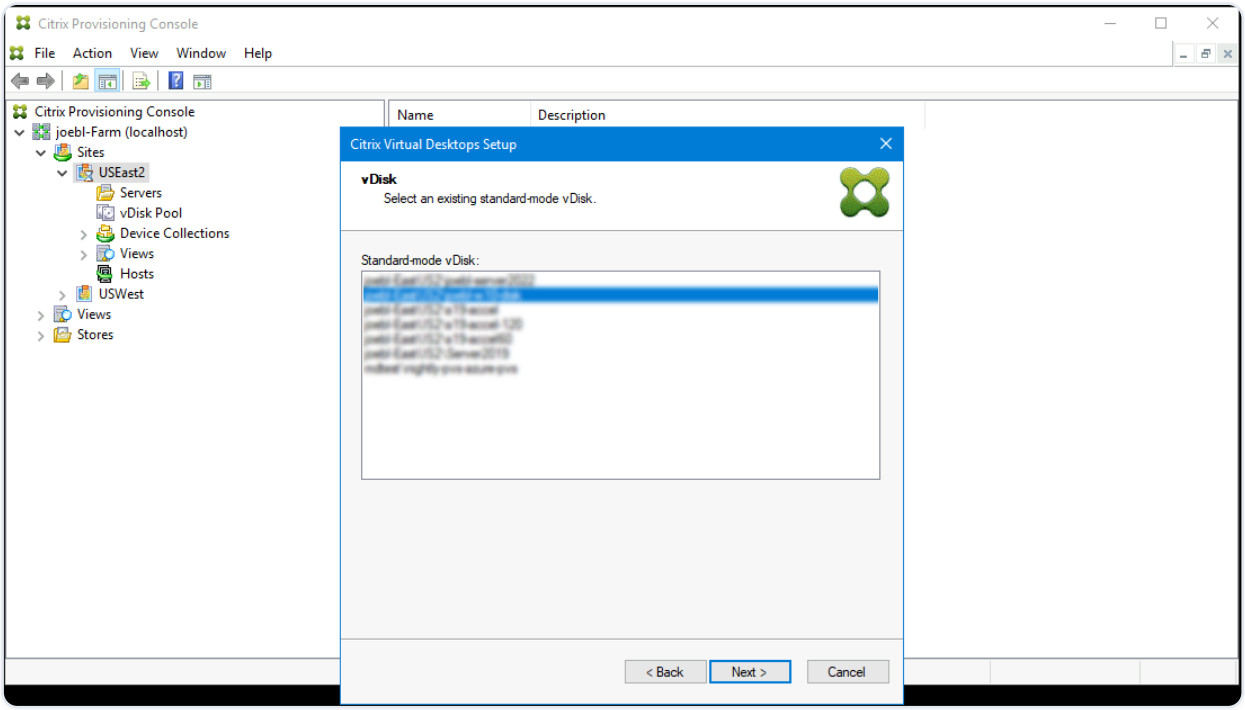
Click **OK** to return to the authentication page.

5. Choose a VM previously setup with the settings for the provisioned targets. Template VMs that use a machine size that supports Gen2 VMs are loaded.

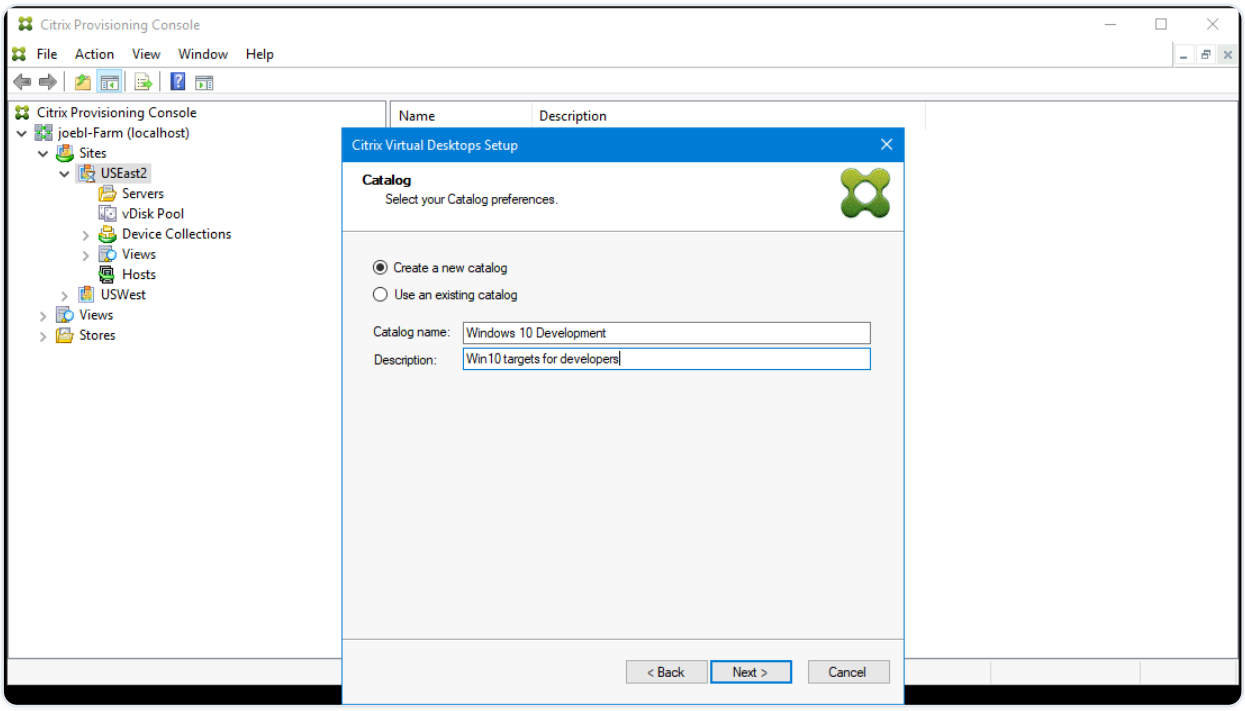


a. Select a VM to use as the template. Choose the same VDA version that you use for on-premises Citrix Provisioning and MCS. Click **Next**.

6. Choose the vDisk to for the provisioned targets.

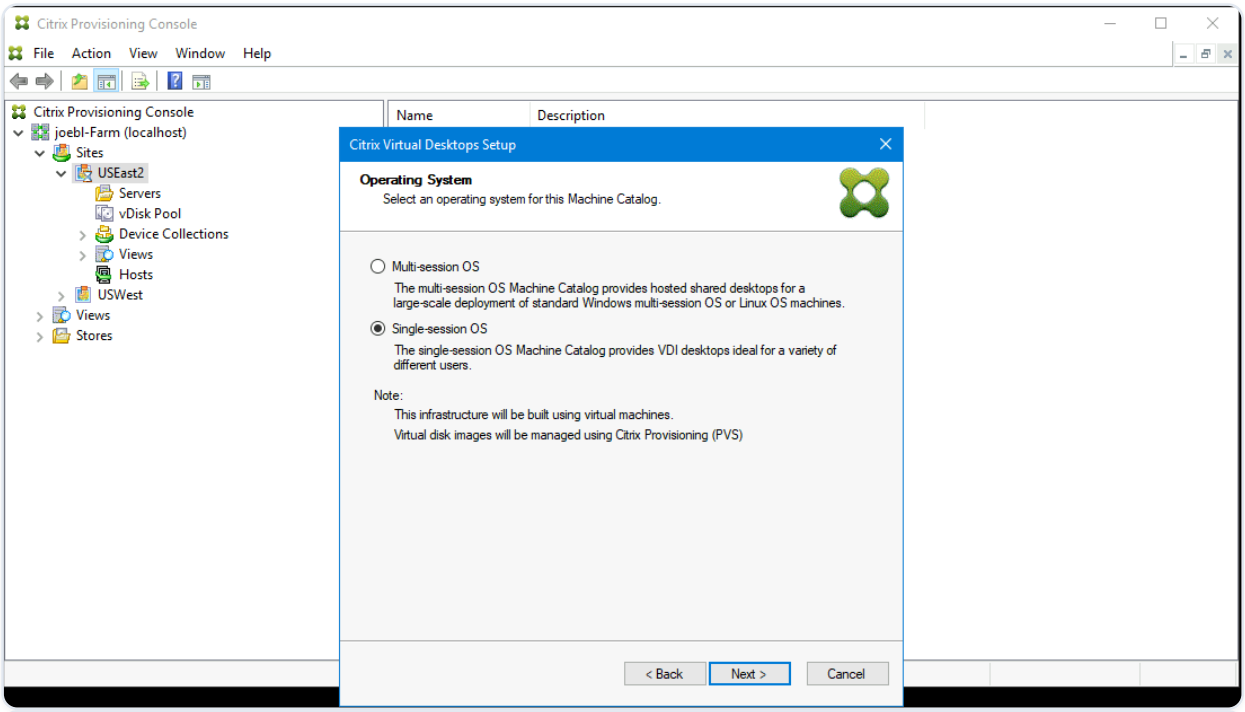


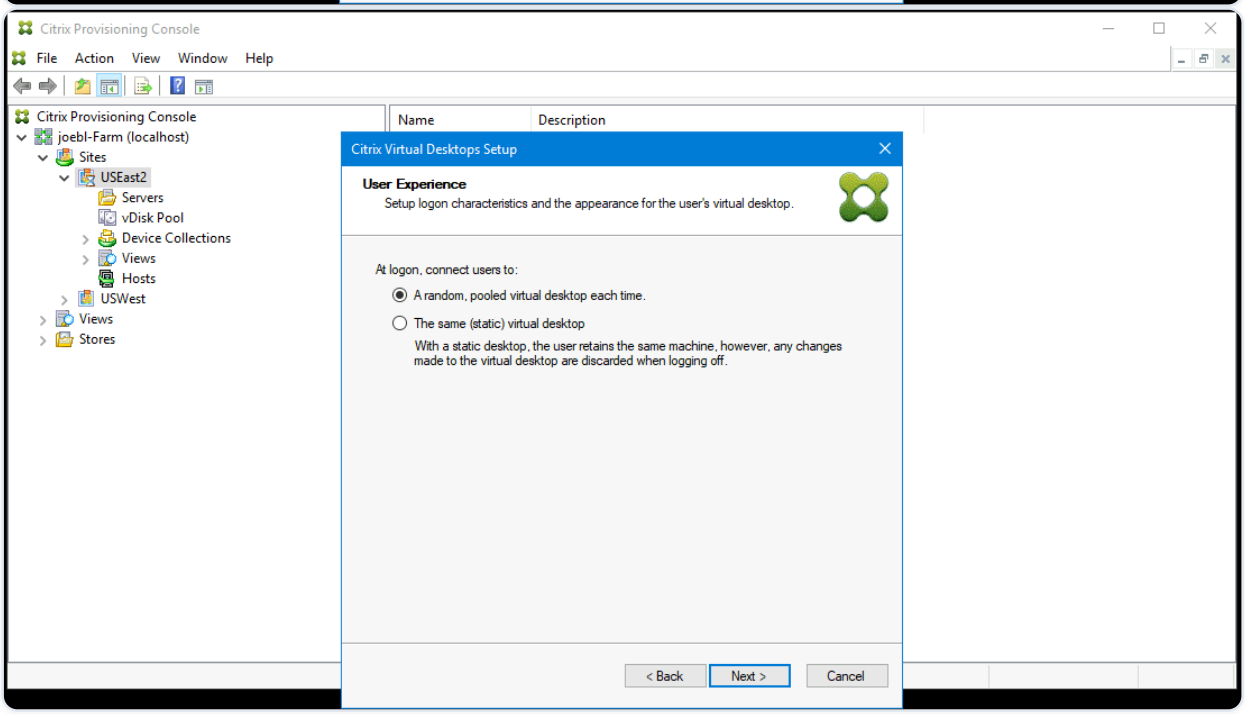
7. Choose to create a catalog, or add the VMs to an existing catalog.



If you add to an existing catalog, a drop-down list of catalogs is supplied for you to choose from.

8. Choose the type of VDA and catalog:





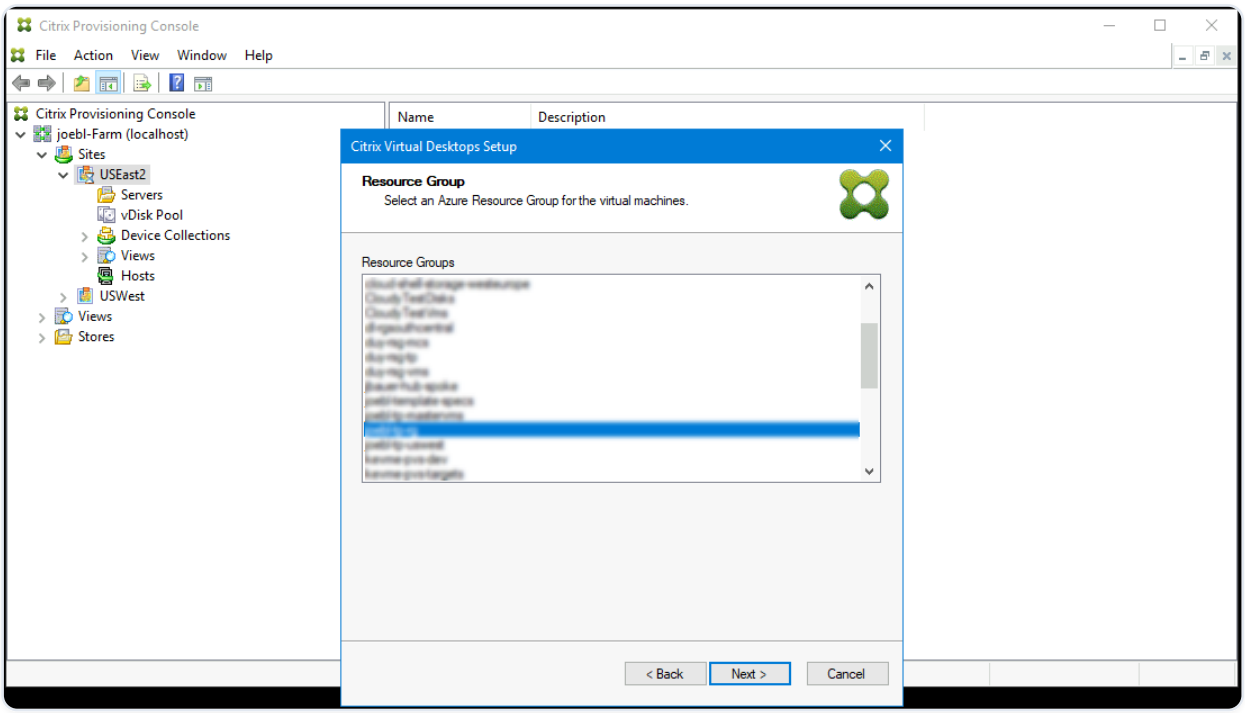
9. On the **Virtual machine**s page, select VM preferences. Preferences vary depending on the machine OS type and if assigned user changes are discarded after the session ends. For a Windows Client or Windows Server machines that are randomly assigned to users:

   - Enter the number of VMs to create (default is 1).
   - Enter the number of vCPUs (default is based on the previously selected template).
   - Enter the memory size. If the template has dynamic memory configured, two extra configuration settings are required (minimum and maximum memory).
   - Enter the local write cache disk size (default is 6 GB).

- Select the checkbox Targets uses IPv6 if you want to create targets that stream using IPv6.

> **Note:**
>
> BDM Mode is the only supported boot mode on Azure.

10. Select the resource group to use when creating target VMs. The resource group must exist, but you determine how the VMs are allocated to resource groups. In the following example, there is a separate resource group for targets, making it easier to manage all targets as a group.



11. Select Active Directory for the targets.

    Citrix Provisioning supports provisioning of target devices in untrusted domains.

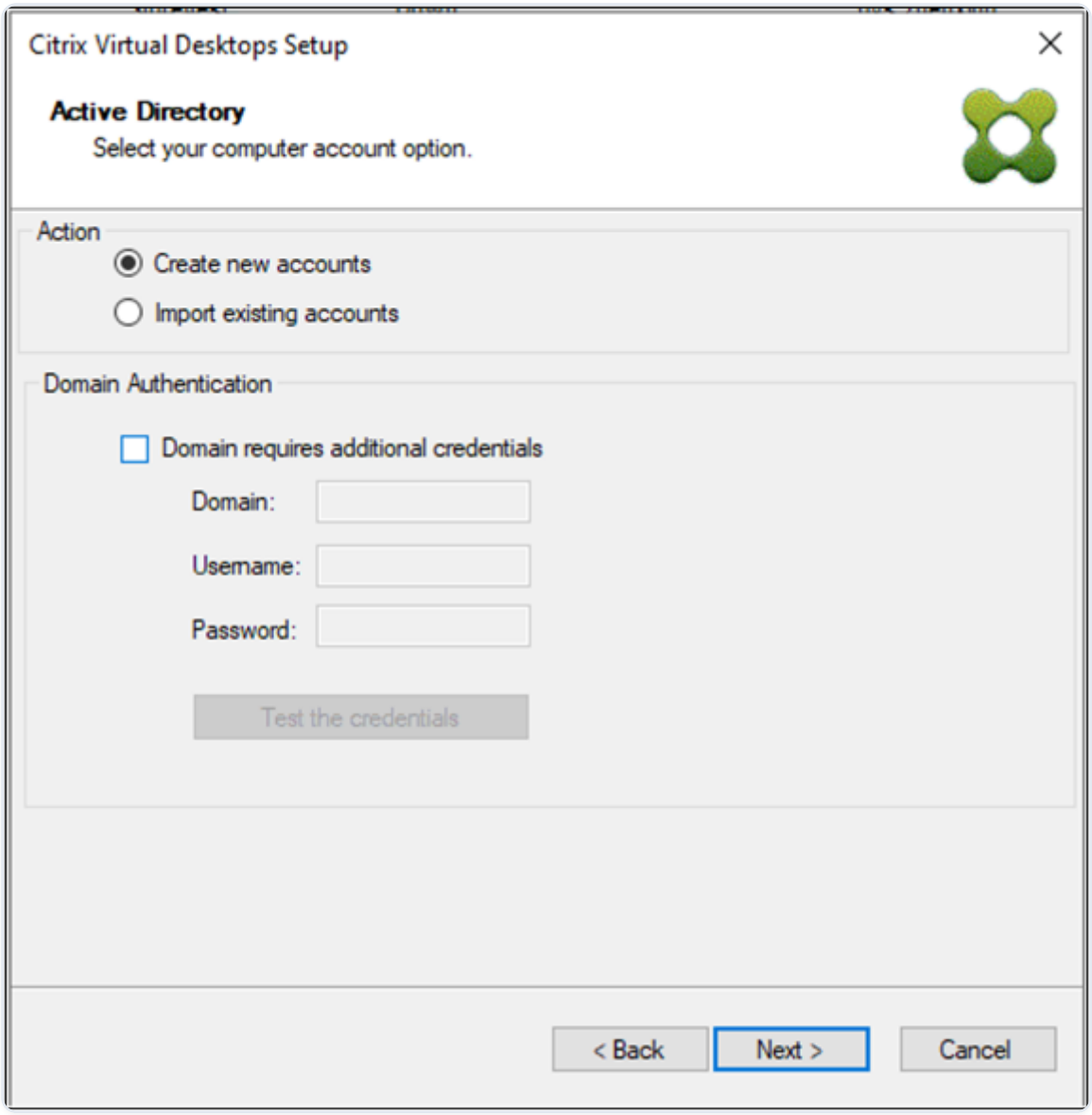
    If the domain is not trusted, under **Domain Authentication**, do the following:

    a. Select **Domain requires additional credentials**.

    b. Enter the domain name, username, and password for the untrusted domain.

    c. Click **Test the credentials**. This action validates the domain name and the credentials.

    d. After you get a green check mark, proceed to the next page.



Note:

Searching Azure Active might take a long time, which can cause the Provisioning Console to stop responding. If the wizard stops responding and a dialog appears with the choices **End Now** or **Cancel**, click **Cancel** to continue with the setup operation.

12. Set up the information about the provisioning servers that function as login servers for the targets. You can select:

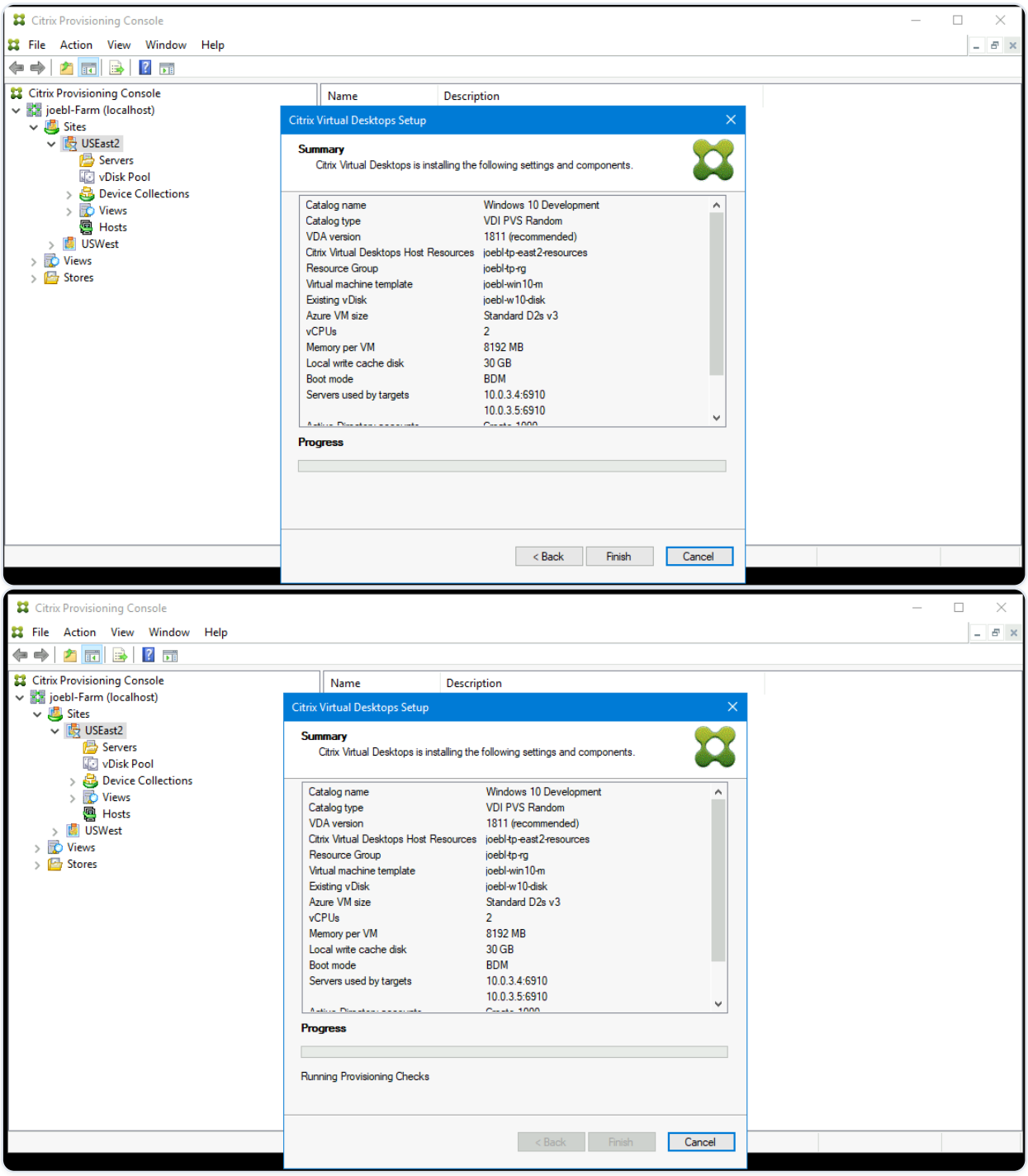
    - **Use DNS to find Citrix Provisioning Servers**: If you have one single Citrix Provisioning Server, then you can use its DNS hostname. If you want a single DNS name to translate to multiple PVS servers, then you have to manually add the records with the common name and the IPv4 or IPv6 address of each server.

> **Note:**
>
> If you want to use a DNS name, then you must specify the fully qualified domain name. DHCP server does not include the zone where you add the DNS name to be used.

- **Use specific servers**: To specify the desired servers by IP address, click **Add** to select from the list of configured servers. Select the servers and click **Add**. The selected servers appear on the **Citrix Provisioning server information** page.

  > **Note:**
  >
  > The IPv6 addresses are displayed if you select **Targets uses IPv6** checkbox earlier on the **Virtual Machines** page.

13. Verify the information on the summary page, and click **Finish** to begin the provisioning process.



Also, consider the following:

- After clicking **Finish**, the Citrix Virtual Apps and Desktops Wizard does a pre-flight check. Citrix Provisioning runs tests to verify that enough resources (CPUs, NICs, and IP addresses) exist. An error message appears if the pre-flight check fails.



- During the Citrix Virtual Apps and Desktops Wizard process, the newly created VM boots up to format the write cache disk, then shuts down. This process takes a few minutes. If the machine times out during this operation, the setup process fails.
- By default, 200 VMs are created in a batch operation.

Manually creating target VMs on Azure

Citrix recommends using the Citrix Virtual Desktops Setup Wizard to create target VMs and integrate with Citrix Virtual Apps and Desktops and Citrix DaaS, as documented in the previous section. If you cannot use the Citrix Virtual Desktops Setup Wizard, then you can manually provision target VMs using the procedures outlined in this section.

The Citrix Provisioning Server and targets do not support either PXE or ISO boot on Azure, because Azure does not support them. Instead, target VMs boot using a small boot disk, the BDM Boot Disk, which is about ~20 MB and contains the Citrix Provisioning UEFI boot application.

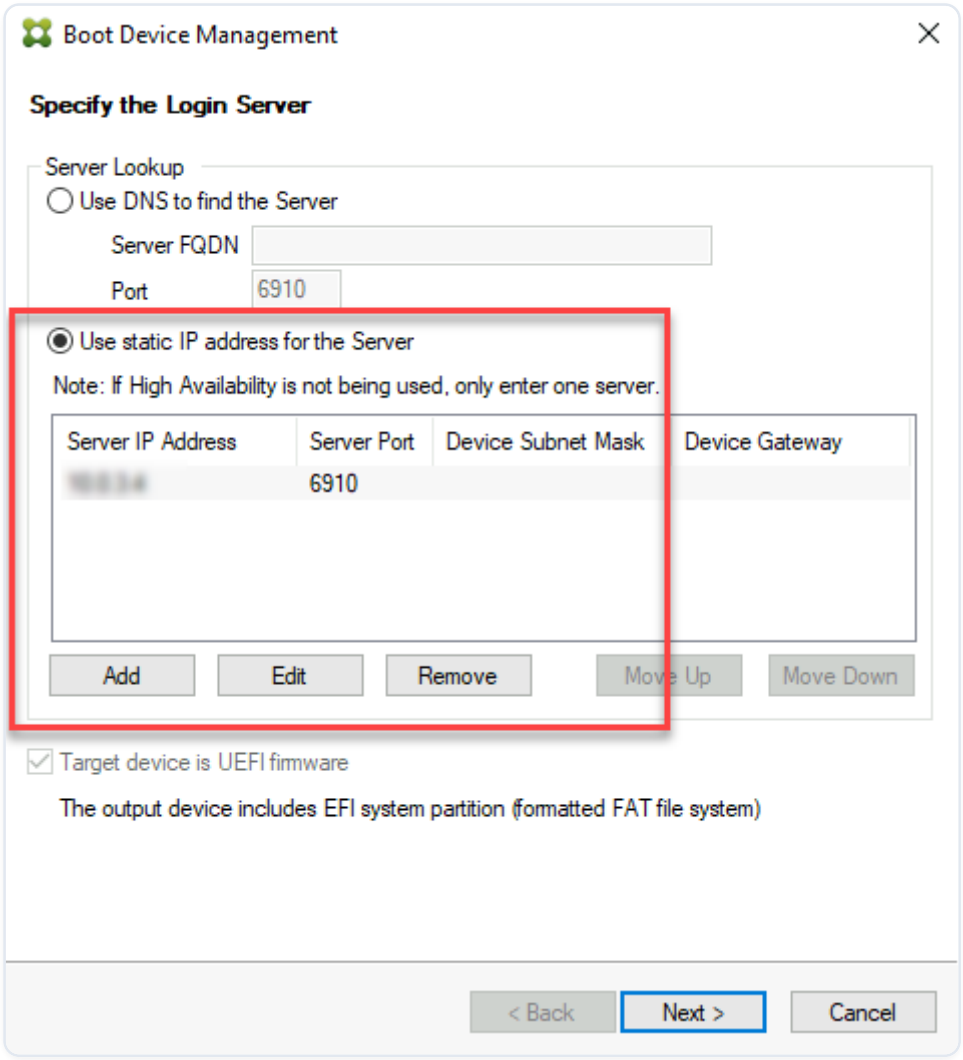
Creating the boot disk

Create the boot disk using the **Boot Device Manager (BDM)** program installed with the server. Run as follows:

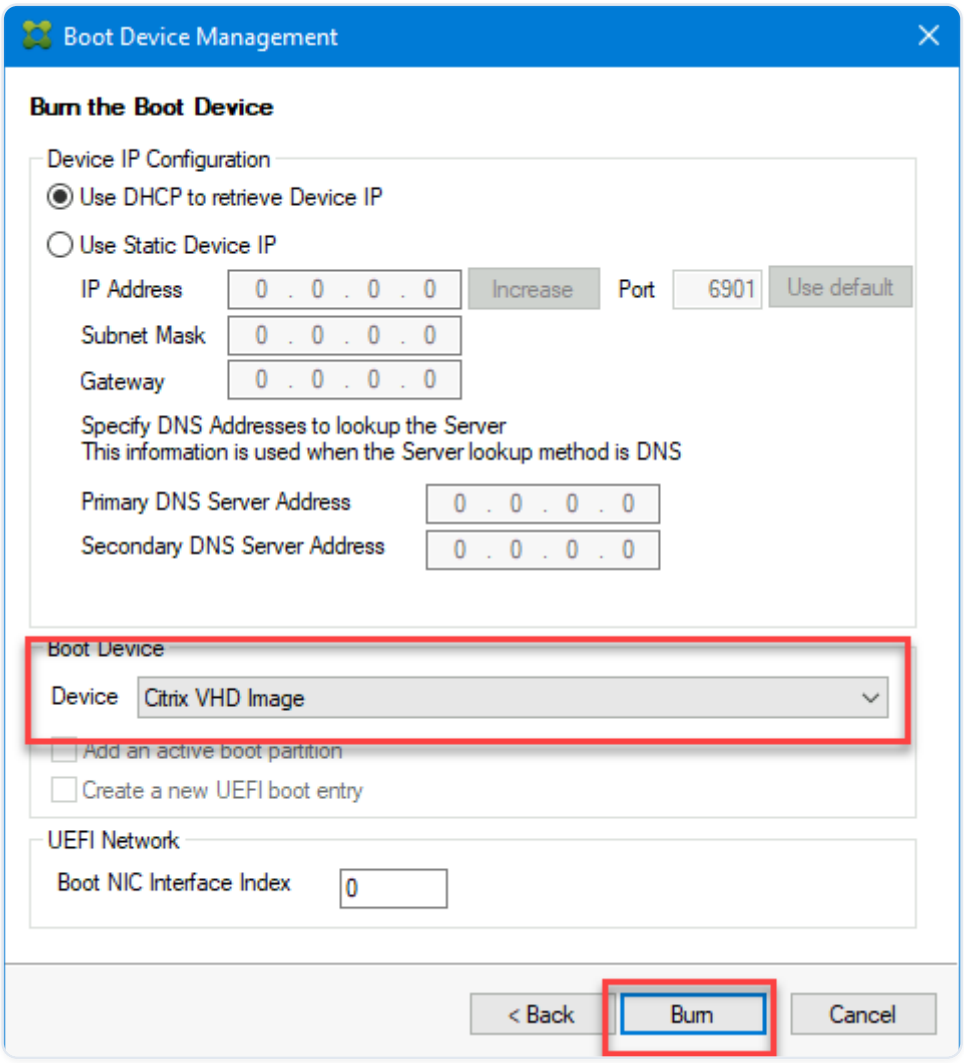
1. Run the **BDM.exe** program.

   ```
   C:\Program Files\Citrix\Provisioning Services\BDM.exe.
   ```

2. Specify the Login Server: Enter the Provisioning Server information.



3. Create the boot disk VHD file: In the **Device** field, select **Citrix VHD Image**, and click **Burn**.



Target VMs can also use a DNS name to locate the Provisioning Server, as opposed to specifying its IP address. First, you create a DNS entry that maps to the IP addresses used by the Citrix Provisioning servers on the streaming network. Then, you configure the BDM Boot disk to contact your Citrix Provisioning servers using this name.

Defining the DNS name to locate the Provisioning Server is useful for High Availability (HA), because it allows you to return a list of IP addresses as opposed to configuring all IP addresses in the BDM boot disk. To use this feature, you create a DNS entry that maps to one or more IP addresses used by the provisioning servers on the streaming network. In this case, you run the **BDM.exe** program, and specify the DNS host name for the provisioning server DNS on the first page.

Creating the Target VMs

If you want to provision VMs yourself, use the following instructions to create the target VMs:

1. Create the BDM boot disk as outlined above, and upload the boot disk to an Azure managed disk. See Uploading VHD to Managed Disk for instructions on uploading a VHD to Azure.

2. Create target VMs on Azure using the BDM boot disk you created, an empty cache disk of the size you need, and connected to a subnet that has access to the provisioning servers. See Create Target VMs on Azure.
3. Manage the Target devices in Citrix Provisioning. You can manually add each target VM using the provisioning console or use the Import Wizard to bulk import manually provisioned VMs. Use the Azure portal, Azure command line, or Azure PowerShell commands to extract the MAC address assigned to the boot NIC of each manually provisioned target VM.
4. Start each VM once to ensure that the setup is finalized. During this boot, Citrix Provisioning formats the cache disk, and then shuts the VM down. Once it is shutdown, use the Azure portal, Azure command line, or Azure PowerShell commands to deallocate the VM.

> **Note:**
>
> You can choose the resource groups, VNet, and disk types if the network contacts the Citrix Provisioning server and the storage type chosen for the cache disk is standard SSD or better.

Azure server side encryption with customer-managed key

Citrix Provisioning on Azure now supports customer-managed encryption keys to encrypt all managed disks, which are BDM Boot disk and WBC disk, associated with each target device. With this support, you can manage your organizational and compliance requirements by encrypting the managed disks of your machine catalog using your own encryption key. For more information, see Server-side encryption of Azure Disk Storage.

A Disk Encryption Set (DES) represents a customer-managed key. Assign a DES ID to the boot disk of the template VM. This DES is applied to all disks created when targets are provisioned using Citrix Virtual Apps and Desktops Setup Wizard. The disks created also include BDM Boot disk and WBC disk. Also, if you select Encryption-At-Host for the target VM, then encryption starts on the VM host itself. The encryption is also applied to all target VMs provisioned using the Citrix Virtual Apps and Desktops Setup Wizard.

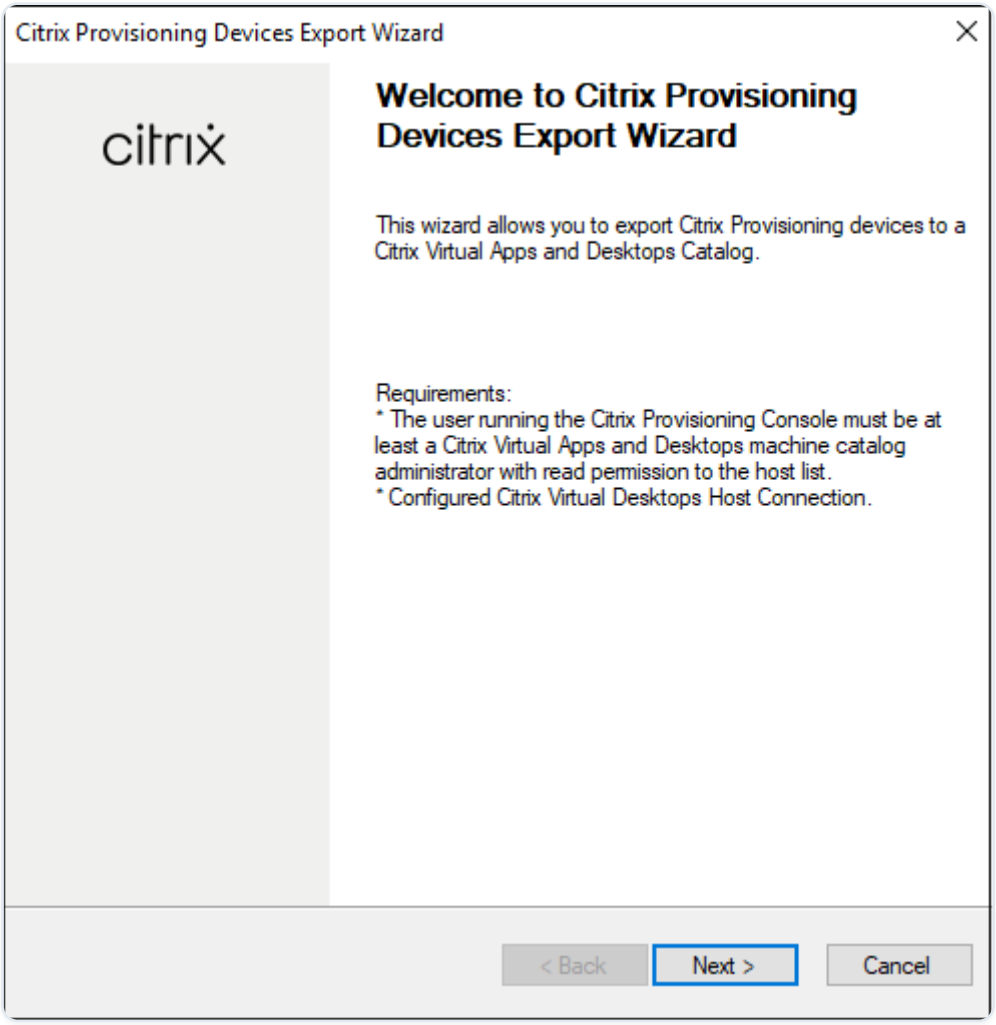
Integrate Manually Created Targets with Citrix Virtual Apps and Desktops and Citrix DaaS

Adding a Hosting Connection in Studio connects you to your resource location. When you specify your Azure credentials, Studio creates an Azure Application ID and secret. Citrix DaaS uses these

Azure credentials to control the VMs in the resource location. The provisioning Export Devices Wizard uses data from this hosting connection to assist it in creating a Broker Catalog.

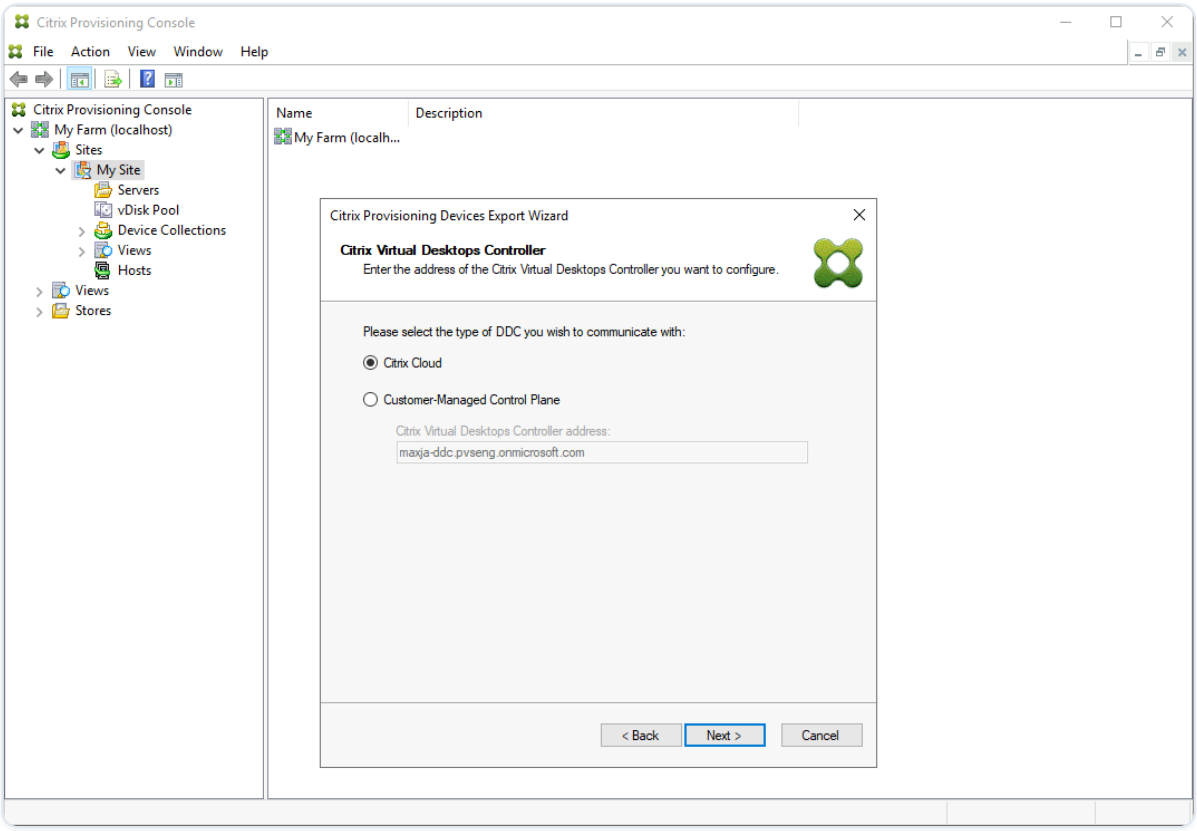
To integrate with Citrix Virtual Apps and Desktops and Citrix DaaS:

1. Launch the **Export Devices** wizard from the Citrix Provisioning console.
2. Click **Next** to start the wizard.

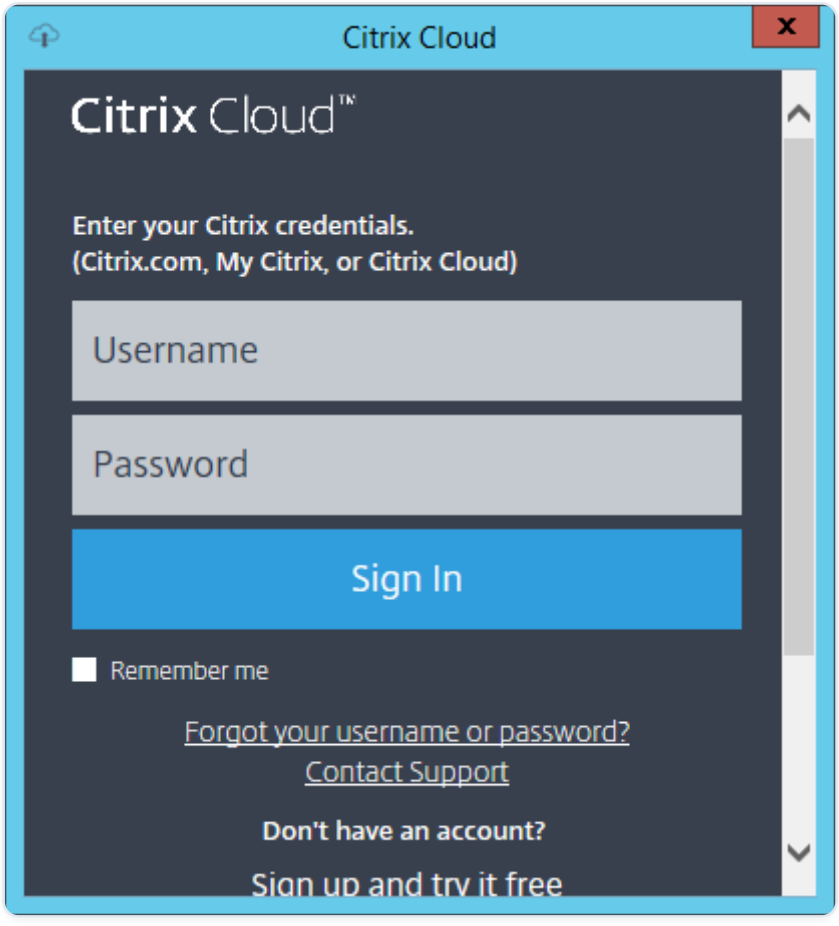


3. On the **Citrix Virtual Desktops Controller** screen, select the type of delivery controller.

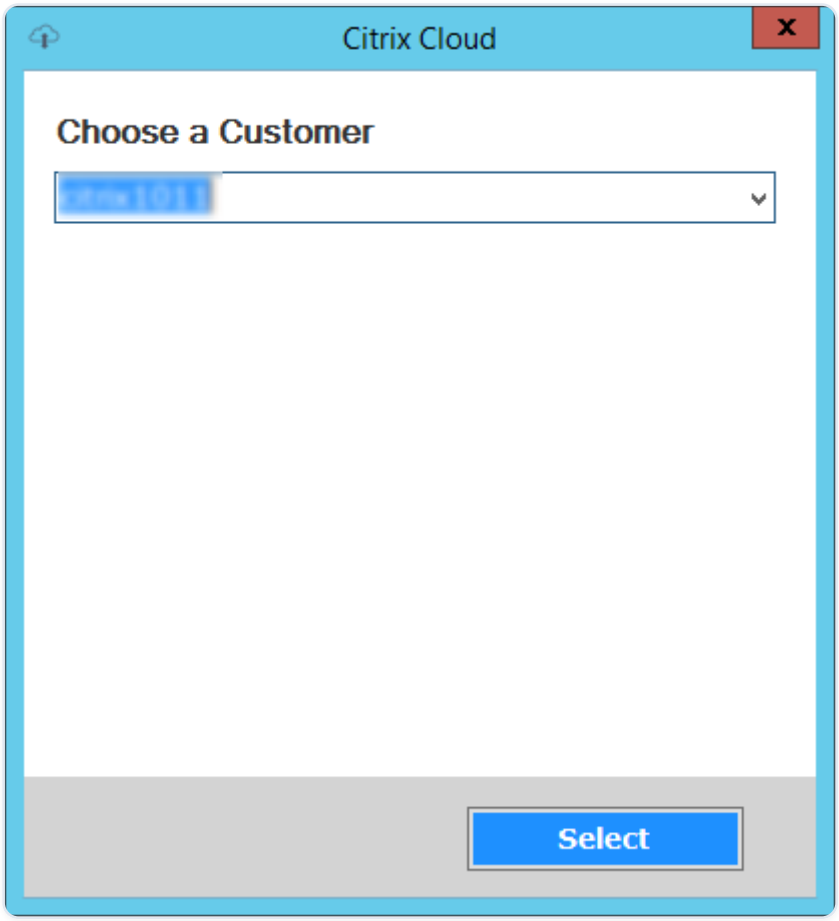
    a. If you select **Citrix Cloud**:



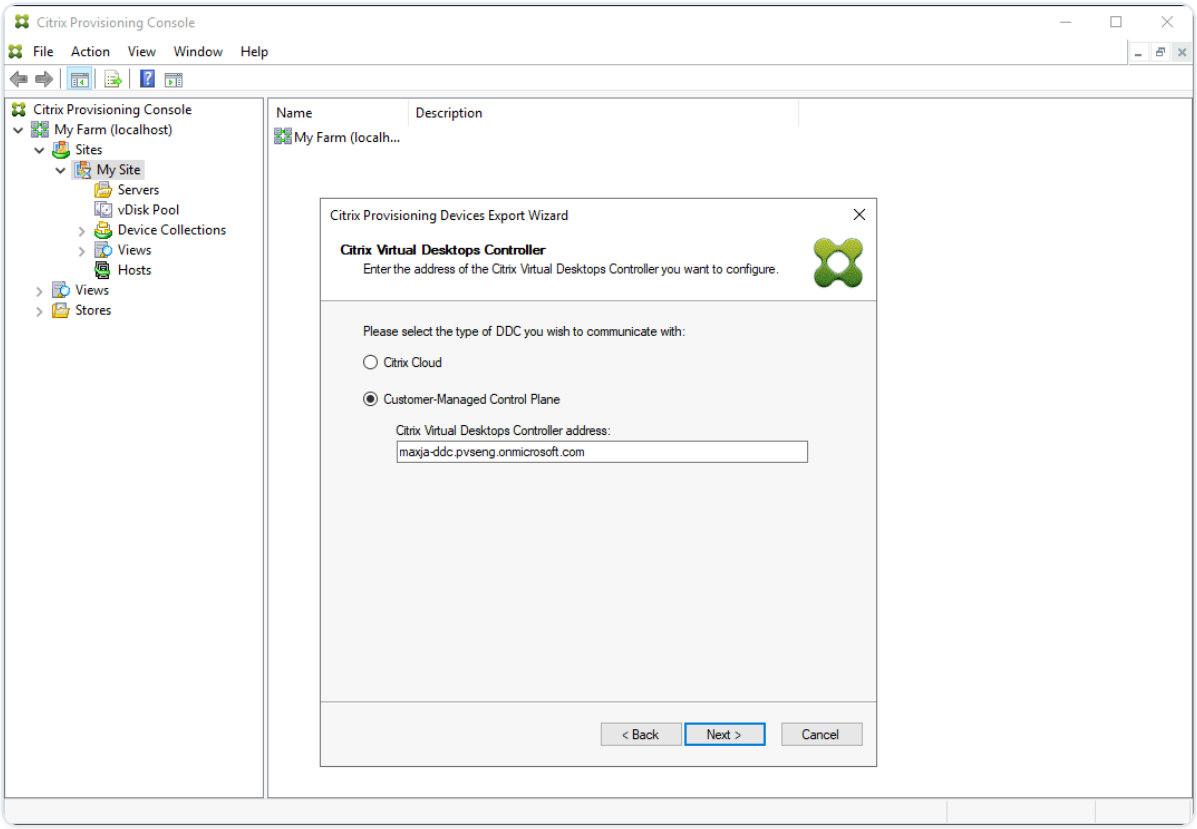
i. Enter Citrix Cloud credentials.



ii. If you have more than one customer, select appropriate cloud customers.

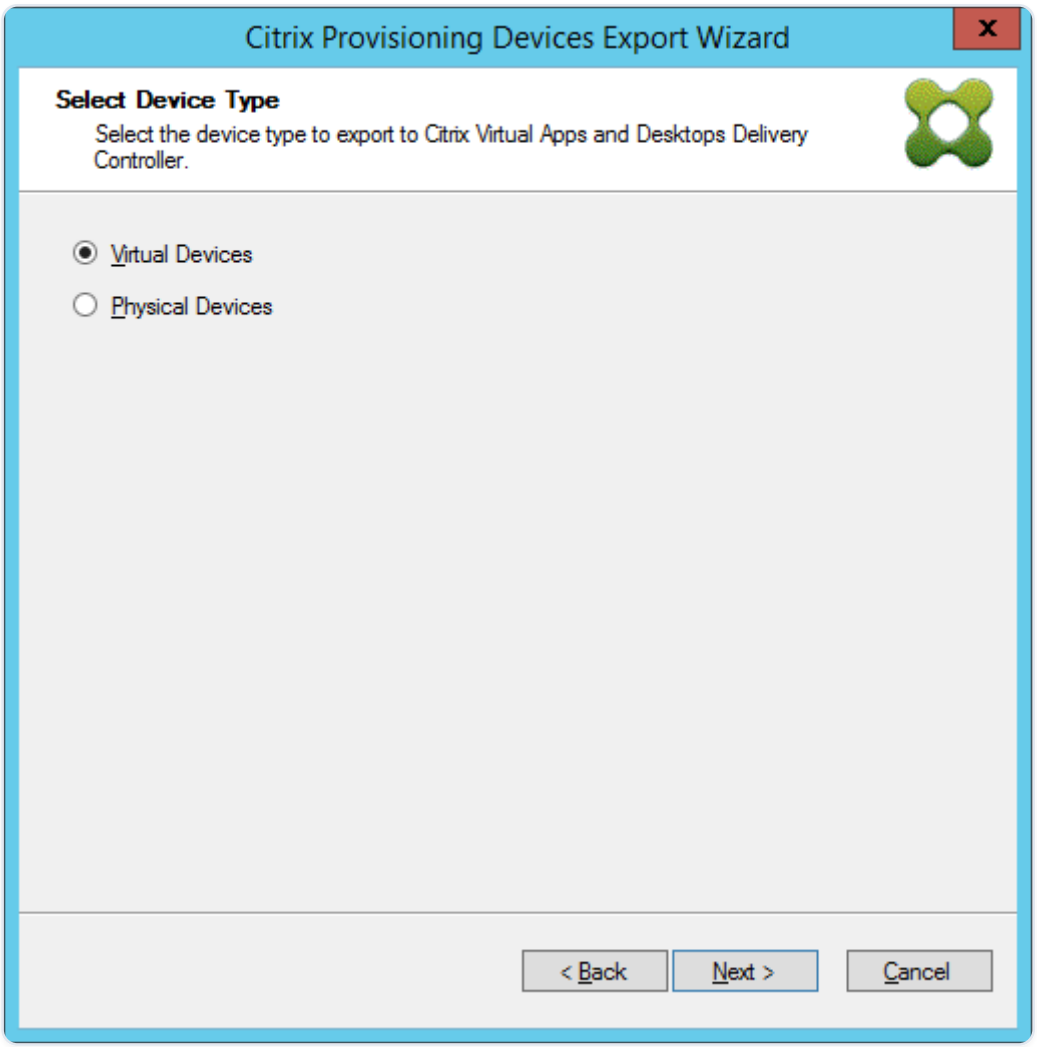


b. If you select **Customer-Managed Control Plane**:



i. Enter the controller hostname or address. The wizard authenticates to the Delivery Controller using the current logged in user.

4. Click the **Device Type** to export. Click **Next**. When selecting **Virtual Devices**, the wizard displays the **Host Resource** screen which allows you to click the host or hypervisor. For physical devices, the wizard skips to the **Active Directory and Collection** selection screen.



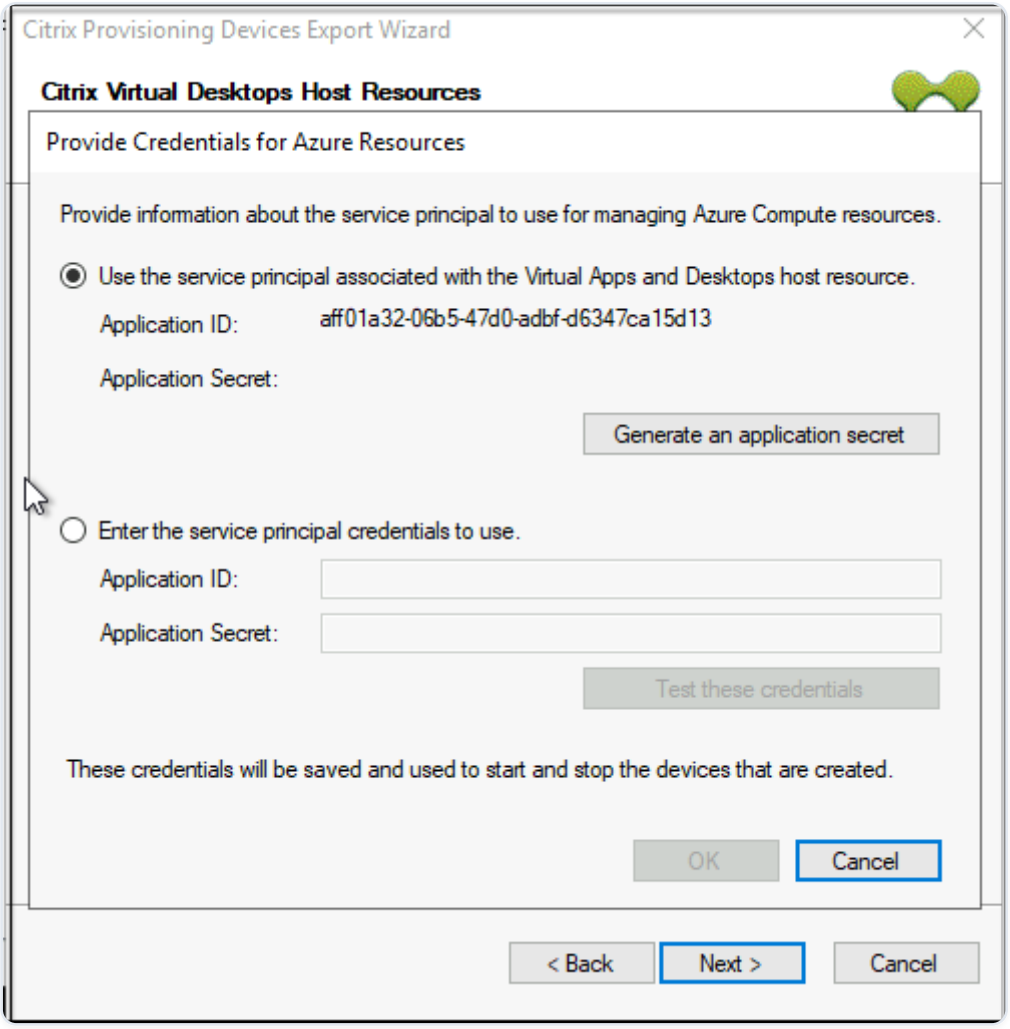
5. On the **Citrix Virtual Desktops Host Resources** screen, select Azure hosting unit. Click **Next**.
6. Establish a Service Principal (SPN) for working with the Azure APIs. An SPN has two components:

   - The Application ID, a GUID uniquely identifying the Service Principal.
   - The Application Secret.

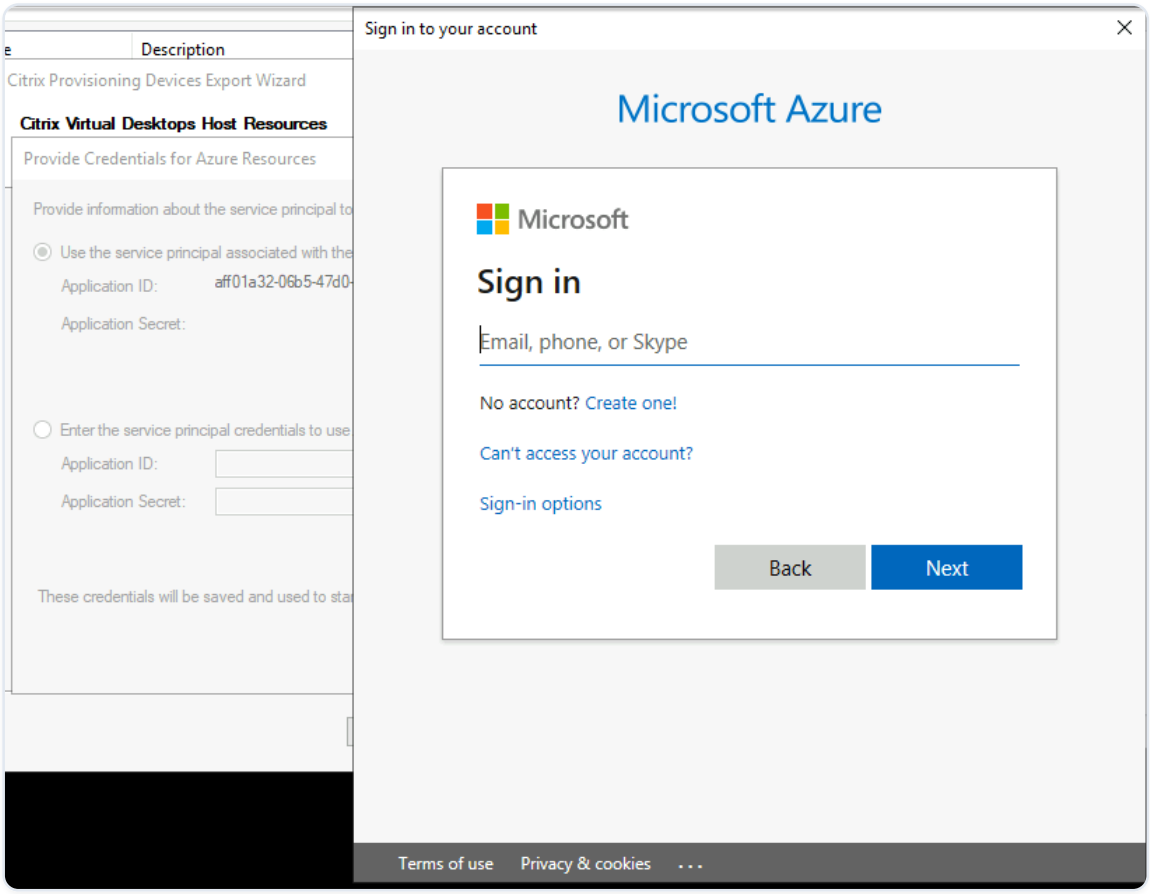
   You have two choices for specifying the SPN:

   - The hosting unit has a configured Application ID. The setup wizard can generate a new secret for this application. However, you need the credentials for the user that initially created the application ID stored in the hosting unit. Continue as follows:

a. Select **Use the service principal associated with the Virtual Apps and Desktops host resource**, and click **Generate an application secret**. The new secret has a validity of one day. The secret is also deleted at the end of running the Export Device Wizard.



b. Sign into Azure using the same credentials used to create the application. If you use different credentials, you get an error.



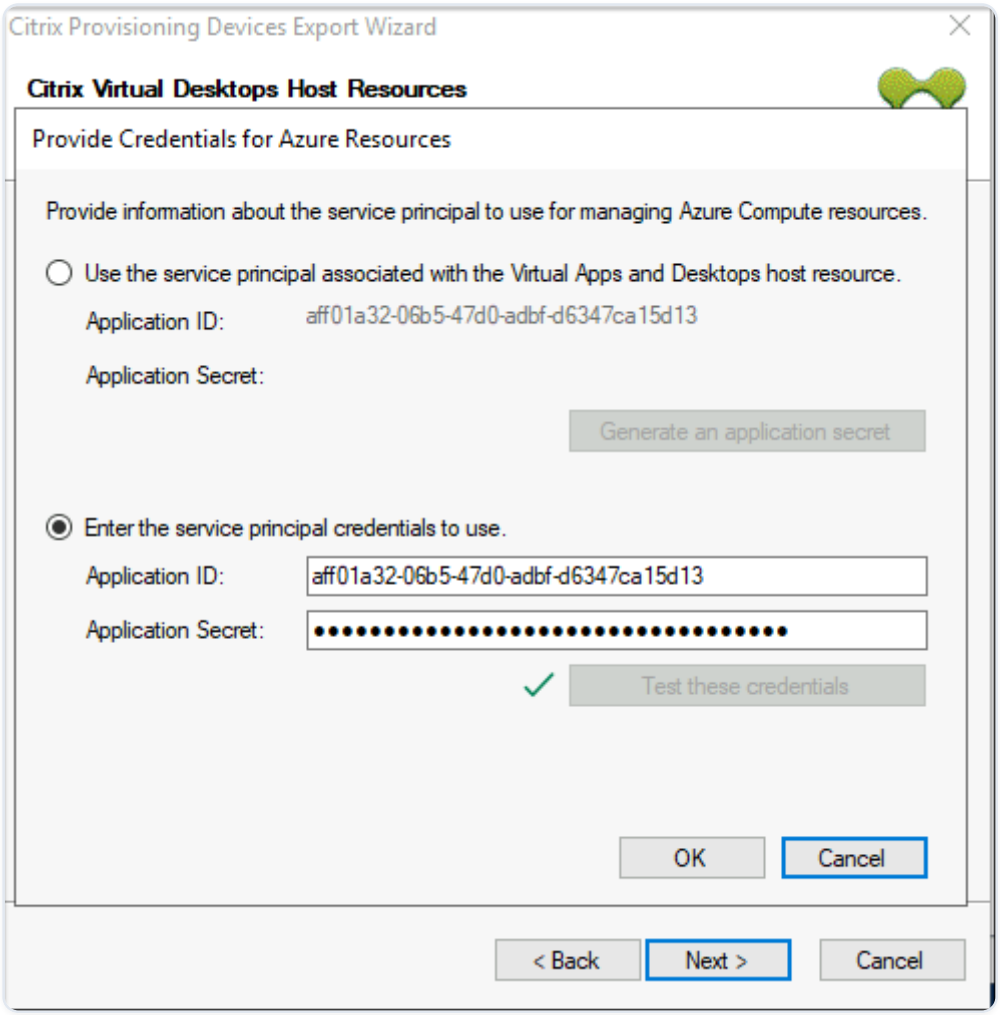
This process can take a significant amount of time. You can press the cancel button to abort if you think it is hung. If you cancel, you are taken back to the screen to generate or enter authentication information.

c. Once successful, the secret is shown as a set of asterisks. Click **OK** to continue.

- If you previously created your own SPN:

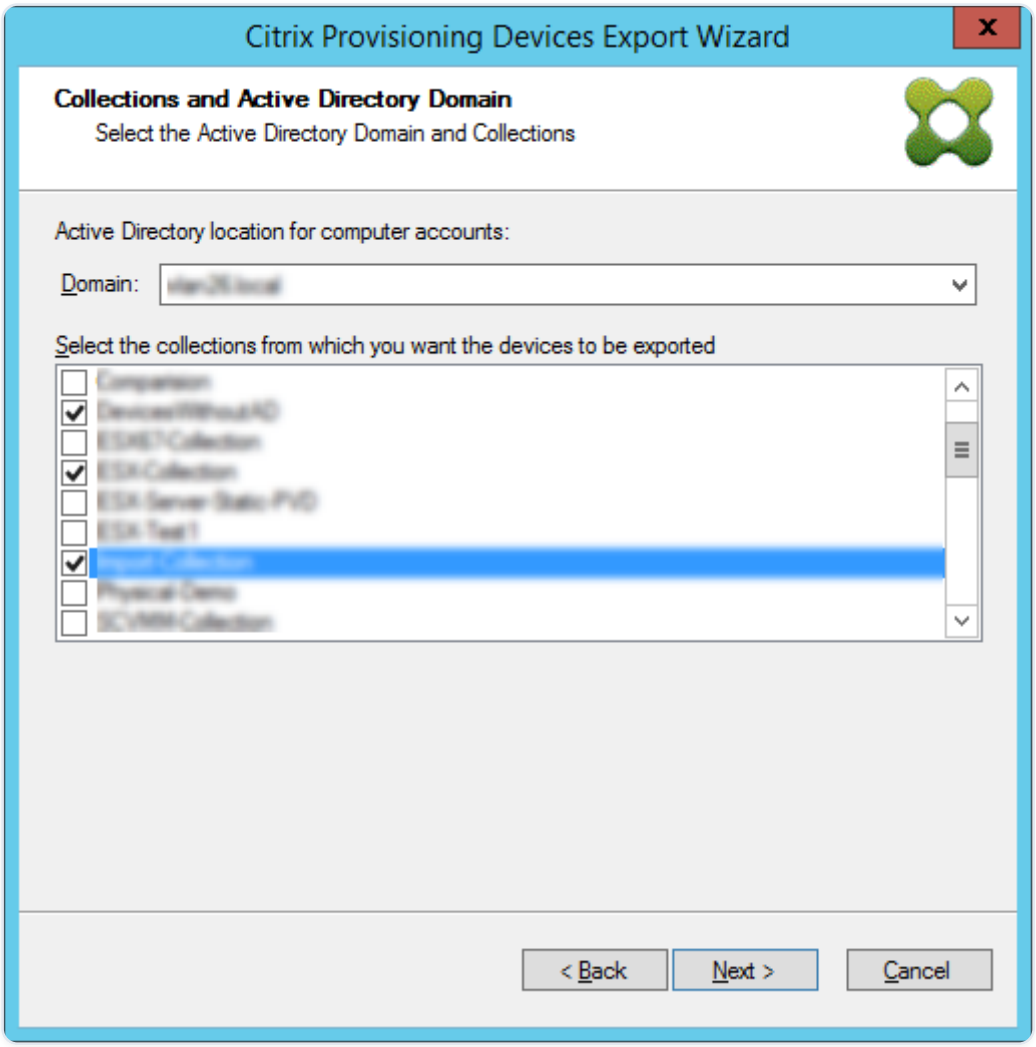
a. Select **Enter the service principal credentials to use**, and enter your application ID and secret. Click **Test these credentials**.

If the SPN is valid, a green check mark is displayed beside the **Test** button.



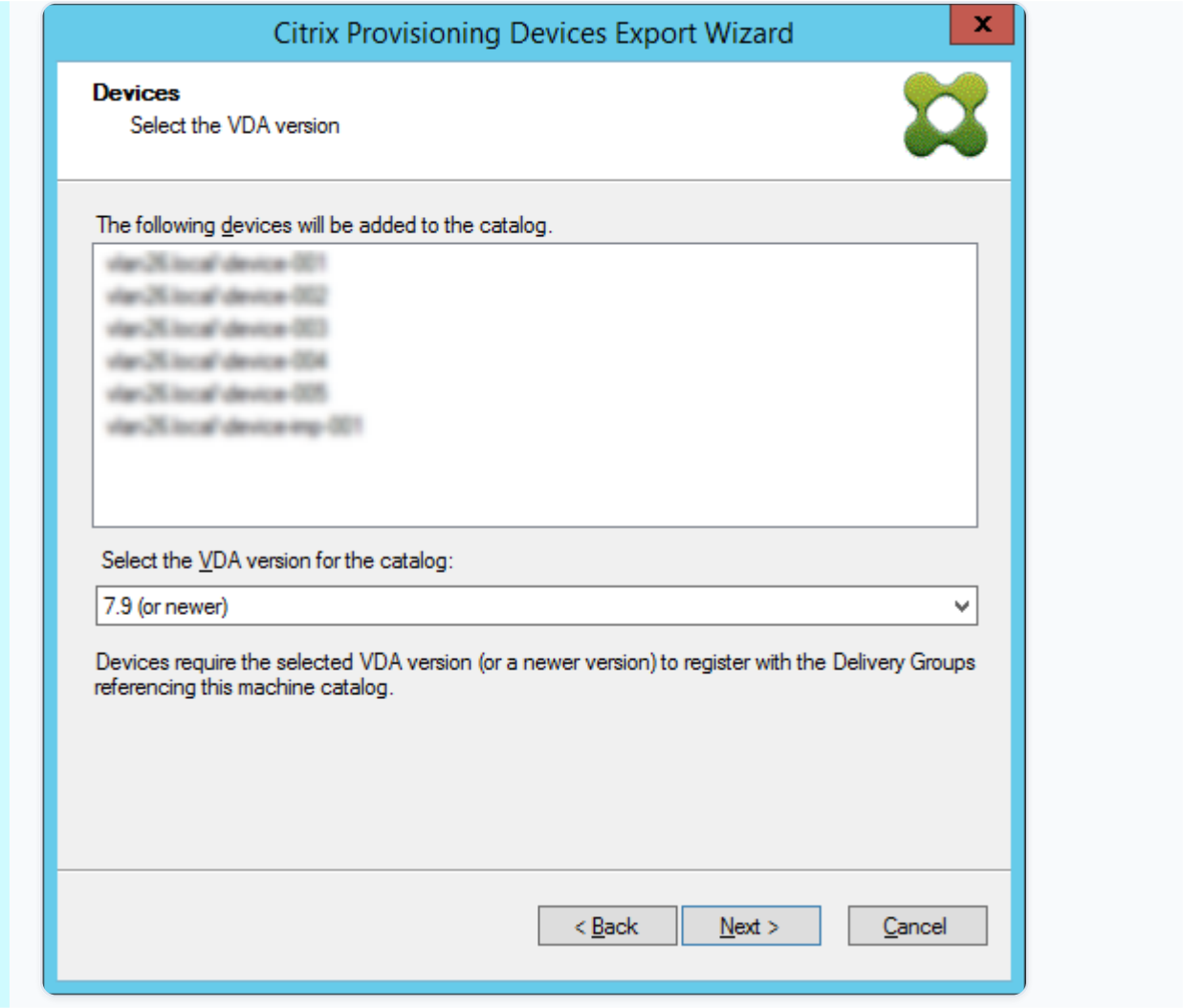
b. Click **OK** to continue.

7. Click the Active Directory domain and collections that you want to export. Click **Next**.

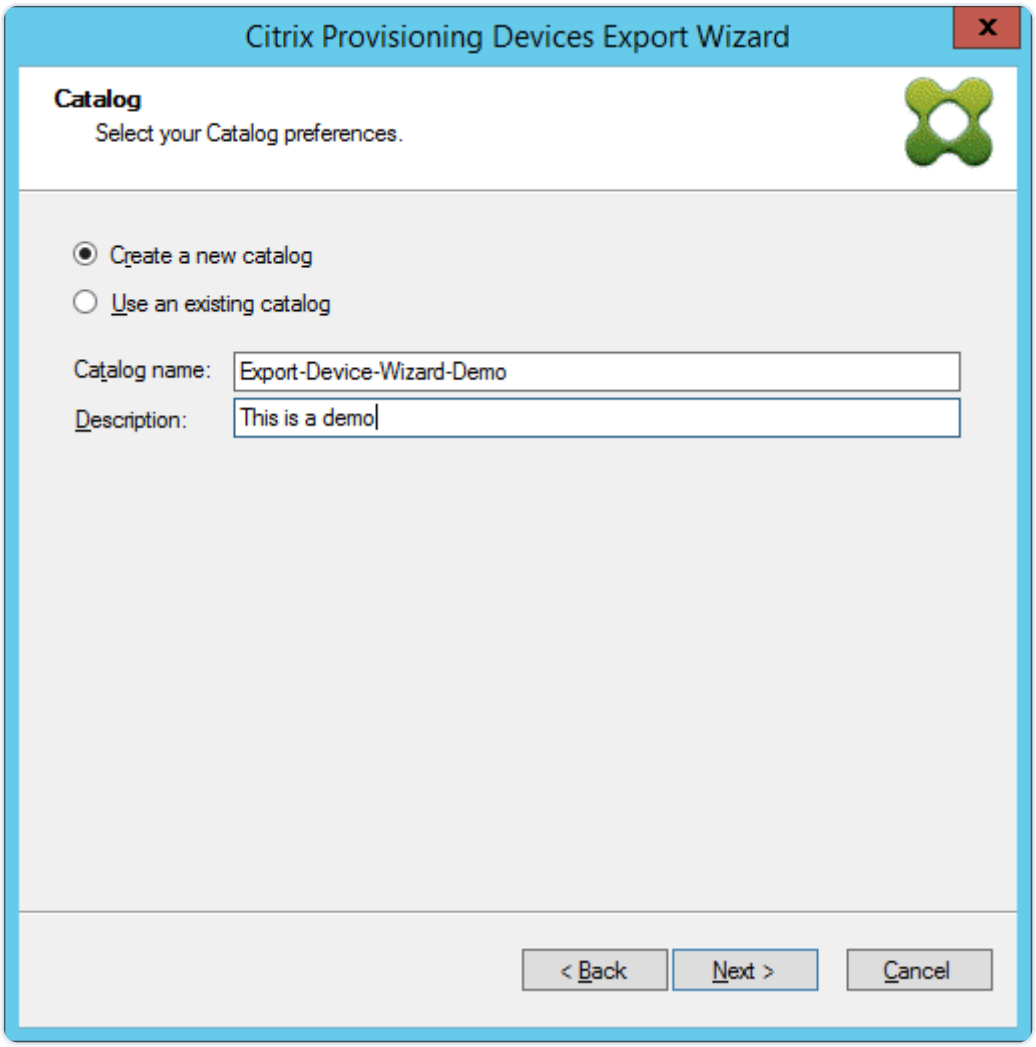


8. Use the list to select the **VDA version**. Devices are required to register with the Delivery Controller referencing the machine catalog. Click **Next**.

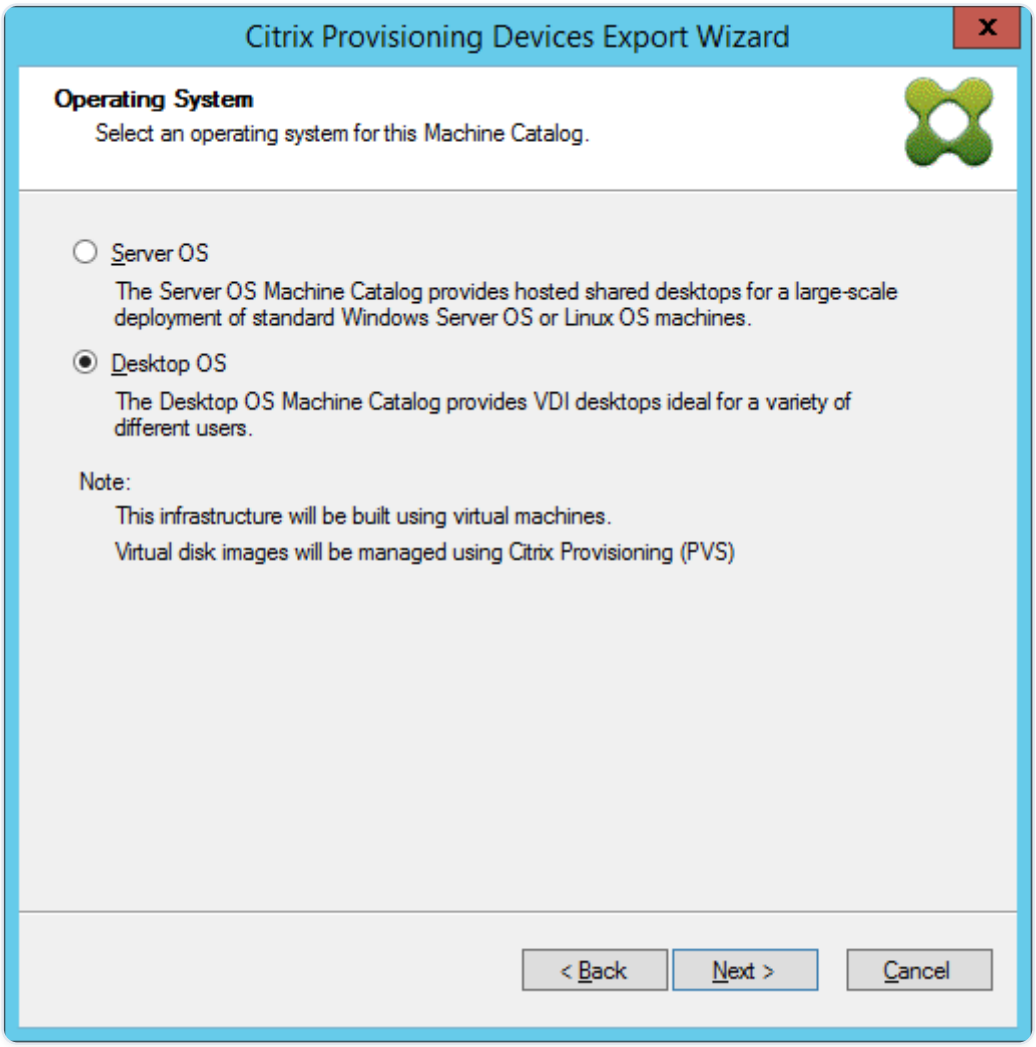
> **Tip:**
>
> All displayed devices are exported to a single Citrix Virtual Apps and Desktops catalog. You cannot select a device in this list.



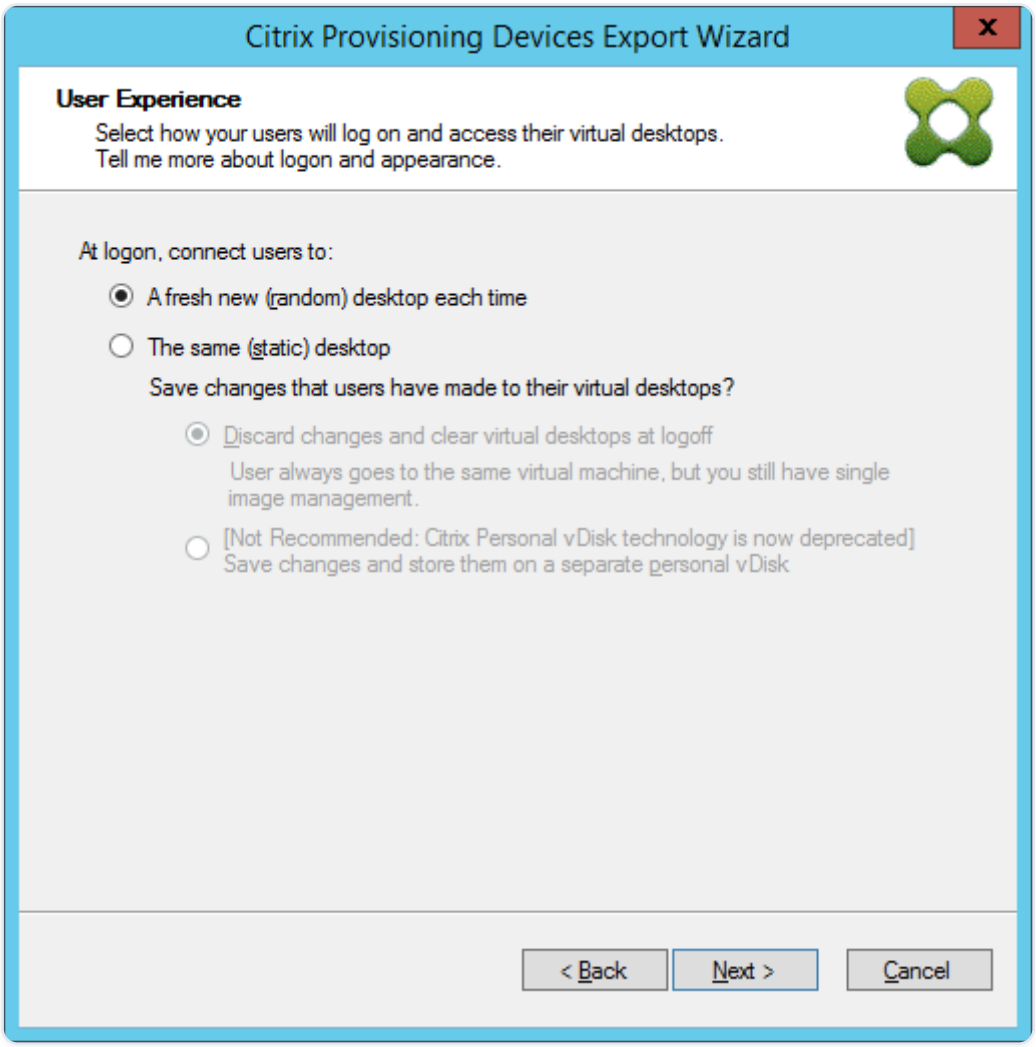
9. Click machine catalog preferences. If you are creating a catalog, specify the name and optionally include a description. Click **Next**.



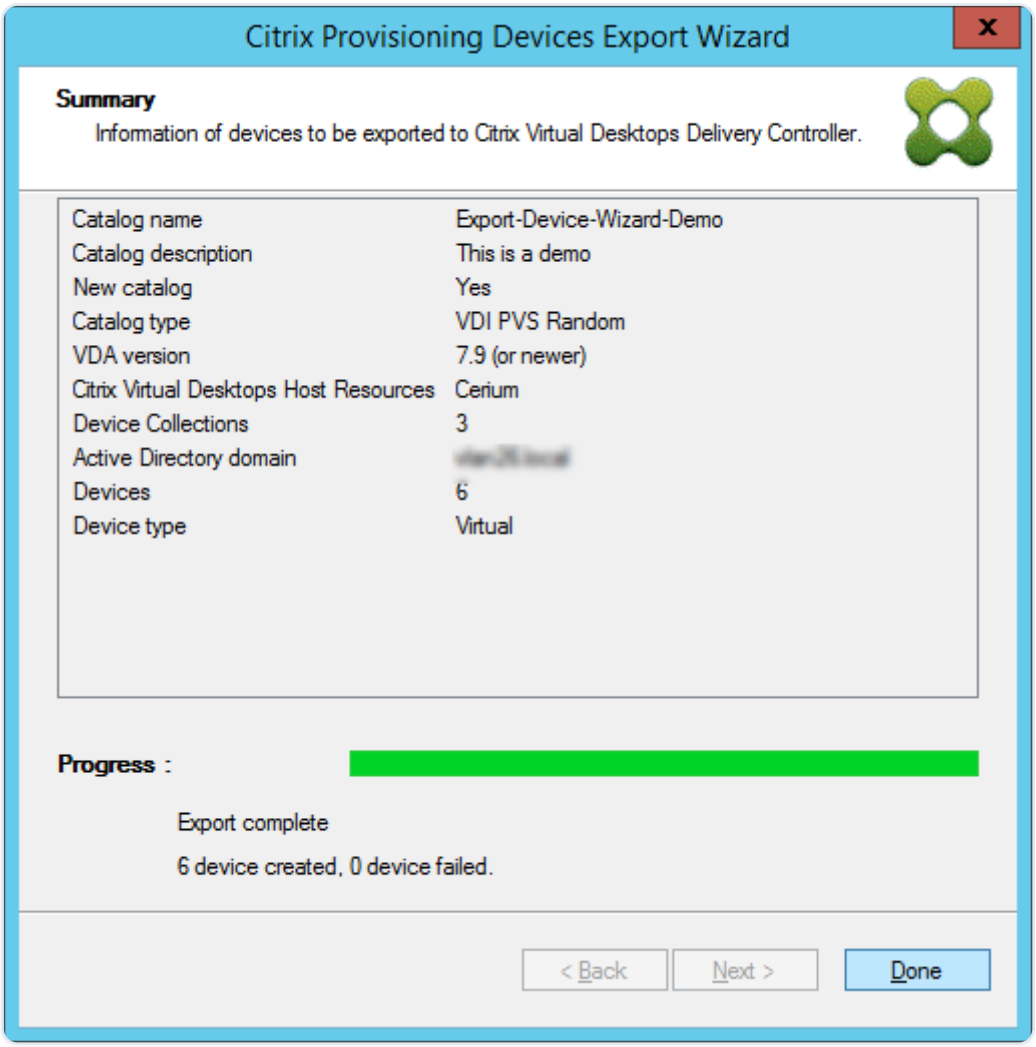
10. Click the operating system. Click **Next**.



11. Set the user experience for the virtual desktop. Click **Next**.



12. Select **Finish** in the **Summary** screen to complete the wizard process.



Note:

The Virtual Hosting Pool data is not added in the Summary screen.

Update Azure credentials

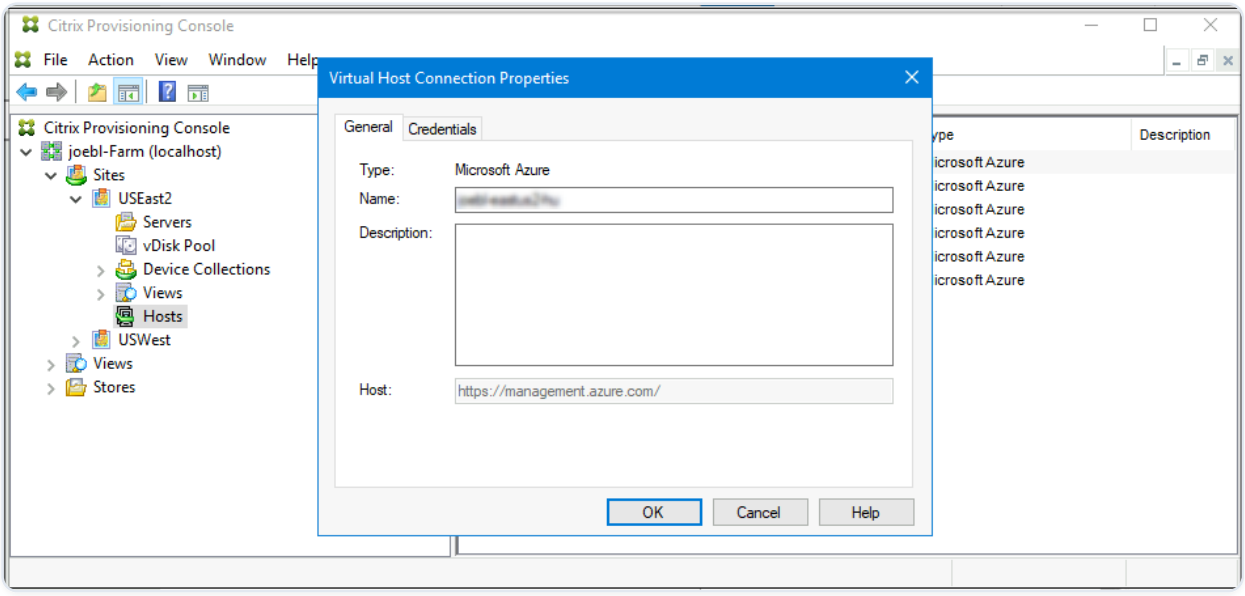
Use the information in this section to update the Azure credentials through the Host Properties in the Citrix Provisioning console.

Note:

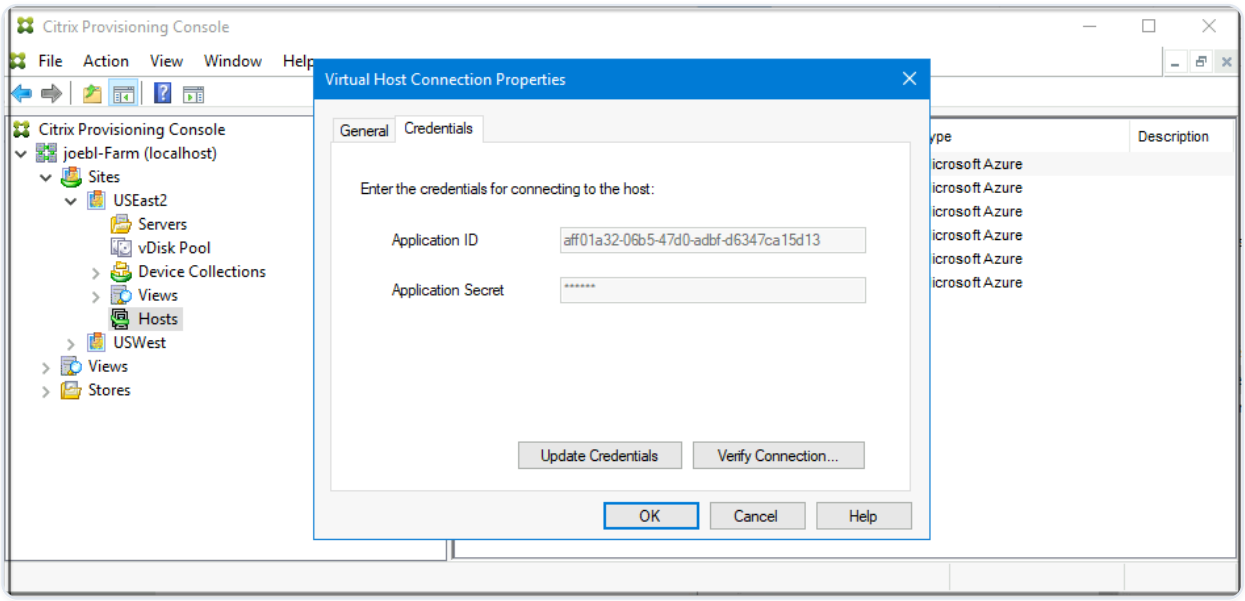
The old secrets are not deleted in Azure when the credentials are updated.

1. In the Citrix Provisioning console, click the **Hosts** node.

2. Right-click the virtual host record to expose a contextual menu.
3. In the contextual menu, click **Properties**. The **General** tab of the Virtual Host Connection Properties is displayed. Ensure that the **Type** is displayed as **Microsoft Azure** for Azure host type.



4. Click the **Credentials** tab. The **Application ID** and **Application Secret** are pre-populated and disabled.



5. Click **Update Credentials** to launch the Azure credentials dialog. You have two choices to update the credentials:

   - **Use the service principal associated with the Virtual Apps and Desktops host resource**

a. Select the option. By default, this option is selected if the Credentials UID is stored in the database.

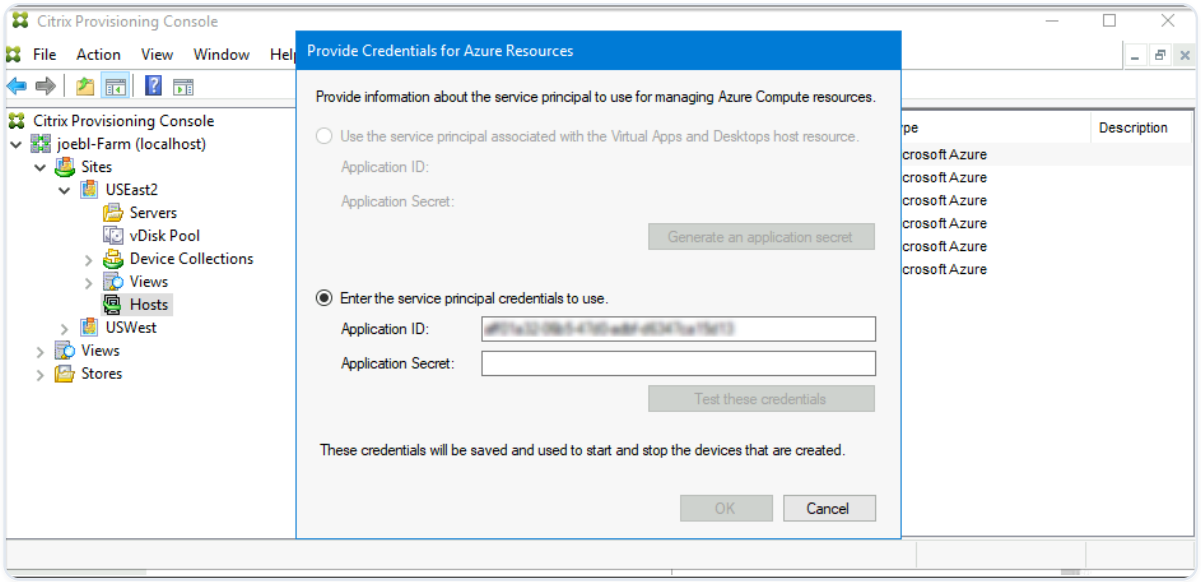
b. Click **Generate an application secret**.

c. Click **OK** when the new secret is generated. On the Host Properties dialog, the **Application Secret** is updated with the new secret. The **Verify Connection** button is disabled.

d. On the Host Properties dialog, click **OK** to save the new credential in the database. If you click **Cancel**, the newly generated secret gets deleted in Azure.

> **Tip:**
>
> The generated secret is valid for one year. The secret is stored in the Citrix Provisioning database and used for power management operations. You can choose this wizard or Citrix Virtual Apps and Desktops Setup Wizard to update the secret when it expires.

- **Enter the service principal credentials to use**



a. Select this option. By default, this option is selected if the Credentials UID is not stored in the database.

b. Enter your application ID and secret.

c. Click **Test these credentials**.

   If the SPN is valid, a green check mark is displayed beside the **Test** button.

d. Click **OK**. On the Host Properties dialog, the **Application ID** and **Application Secret** are updated with the new credential. The **Verify Connection** button is disabled.

e. On the Host Properties dialog, click **OK** to save the new credential in the database.

Delete target VMs on Azure

The delete feature removes the Azure target VMs provisioned through Citrix Virtual Desktops Setup Wizard from the:

- Hypervisor
- Provisioning Server database
- Active Directory account created or associated with the target device
- Machine catalog entries from the Citrix Cloud Connector.

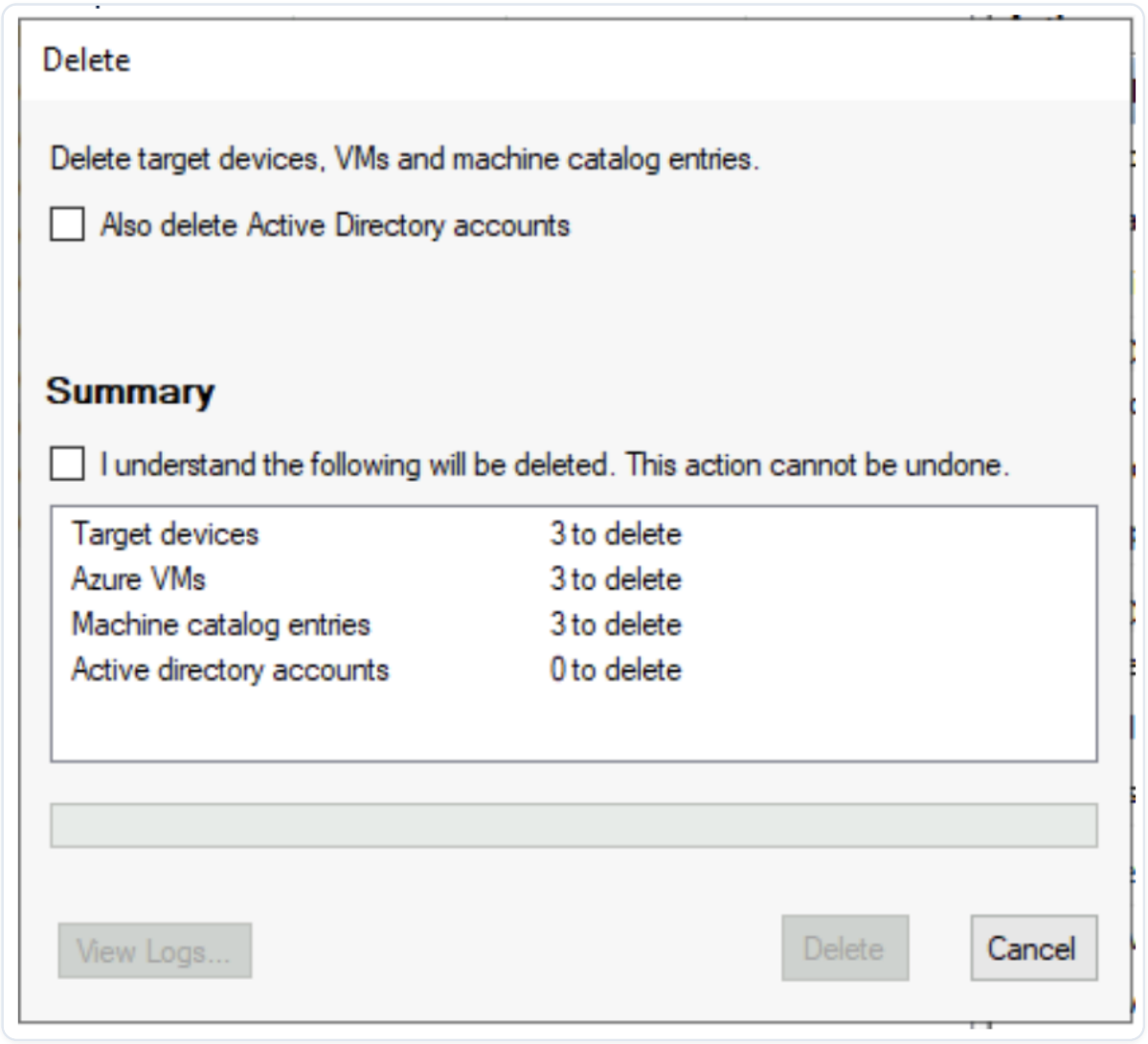
In the Citrix Provisioning Console, you can delete target VMs by individually selecting the devices from the **Device Collections** or **Views**, or delete the entire device collection.

To delete the target VMs:

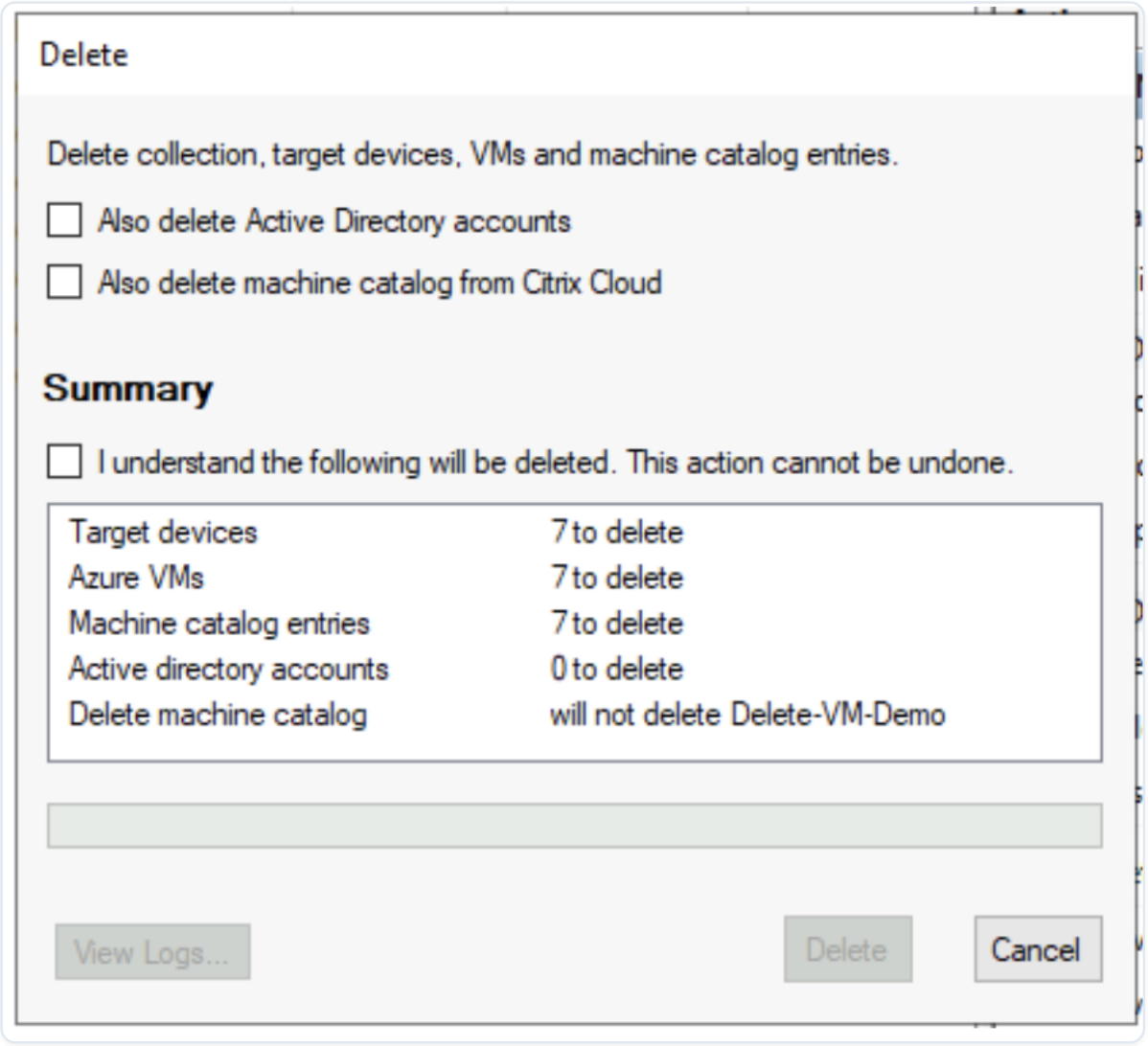
1. Select the devices from the **Device Collections** or **Views**, and right-click to expose a contextual menu.
2. In the contextual menu, click **Delete...**.

> **Note:**
>
> If any of the selected devices are active, an error appears. If you select the devices individually, the **Delete…** option is not available. If you select the entire device collection and click **Delete...**, an error message is displayed.
>
> If any of the target devices is an Azure VM, the following UI is displayed:

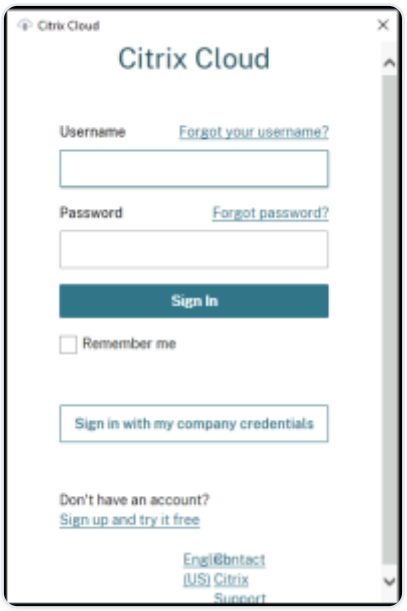
- If you select the devices individually:



- If you select the entire device collection:



3. By default, target devices are deleted from the Citrix Provisioning database, Azure, and the Citrix Virtual Apps and Desktops Machine Catalog. Select the check boxes to delete the device record on other associations. The Summary section is then updated.
4. Click **Delete**.
5. Enter your Citrix Cloud credentials and select the customer.



The Summary text area of the Delete dialog is updated with the status of the deletion.

6. When the delete process is complete, click **Done** to close the Delete dialog. You can also click **View Logs...** to see the status of the delete process or save the log file.

Troubleshooting deletion process

- **Delete...** option is not visible when multiple target devices are selected.

  Verify that the target devices are not active. If they are active, shutdown the devices from the Citrix Provisioning console, and then try again.

- Delete dialog shows Azure VMs deleted, but there are still VMs in the resource group.

  Give Azure some time to delete the VMs. If the VMs are still in the resource group, manually delete the VMs.

- The Machine Entry is not deleted from the Citrix Virtual Apps and Desktops Catalog.

  - Make sure that DDC is responding. You can check by running the following command:

    ```
    asnp citrix.*

    cd XdHyp:\HostingUnits

    dir
    ```

  - Make sure that the SID of the target VM is not missing. You can check by running the following command:

```
Import-Module 'C:\Program Files\Citrix\Provisioning Services
Console\Citrix.PVS.SnapIn.dll'

Get-PvsDevice
```

Check for the `DomainObjectSID`.

- Active Directory record is not deleted.

  If the AD account is deleted from the Active Directory, but the AD record is present on the Citrix Provisioning device, the delete operation fails to find that account and displays an error. Check the AD users and computers and verify that account is present or not.

Citrix Provisioning™ on Google Cloud Platform

This article explains how to move your Citrix Provisioning workloads to the Google Cloud Platform (GCP).

Installing Citrix Provisioning in your Google project is the same as installing it in an on-premises provisioning farm.

Supported features

The following features are supported when provisioning workloads in GCP:

- UEFI boot of GCP VMs.
- Streaming 64-bit Windows Server 2016, 2019 and 2022 target VMs.
- Provisioning target VMs using the Citrix Virtual Apps and Desktops™ Setup wizard.
- Manual provisioning of target VMs using the GCP APIs or gcloud CLI directly.
- Using import wizard to import manually provisioned VMs into the Citrix Provisioning server.
- Using an export wizard to create and update Broker catalogs in Citrix DaaS (formerly Citrix Virtual Apps™ and Desktops service) instances.
- Creating virtual disk from a GCP master VM and updating using either Citrix Provisioning versioning or reverse imaging to the same master VM.
- Manually configuring master VMs to start from the Citrix Provisioning server to do imaging tasks. The imaging wizard automatically configures Master VMs for this task or you can use the `BDM.exe` program.

> **Note:**
>
> Master VMs must be configured to enable UEFI boot time networking. See later section on Master VMs for details.

Limitations

The following features are not supported:

- Windows 10 and Windows 11 desktops. Sole tenant node is not supported. Therefore, only Windows server target VMs licensed by Google can be run.
- In this release, all provisioning target VMs are billed by Google as Server 2019 VMs. A future release will update this to use the license from the original master VM.
- PXE and ISO boot of master and target VMs.
- Legacy BIOS boot of streamed VMs. Only UEFI is supported.
- 32-bit OS support.
- Windows Server release before 2016 are not supported.
- Power management of target devices from the provisioning console.
- You also cannot start provisioned GCP VMs from the Citrix Provisioning console.
- Removal of VMs, catalogs, or AD accounts from Citrix Provisioning console is not supported when Citrix Provisioning is integrated with customer-managed Delivery Controller.

Requirements

To use Citrix Provisioning on GCP, you need the following:

- A GCP project.
- Citrix Provisioning server VM must either use a machine type of e2-standard-4 or above, and SSD persistent disk for boot disk and Provisioning Store disk.
- Access to a Citrix License Server.
- Access to SQL Server: This can be a separate VM running SQL Server 2019, including SQL Server 2019 Express, or Google Cloud SQL for SQL Server.
- To have a better provisioning scale and performance, make sure that the:
  - vDisk has the latest update for Windows

- Citrix Provisioning Server has at least 8vCPUs, 32 GB RAM, and use SSD persistent disk and higher for the vDisk store.

Licensing

The initial product uses the existing licensing mechanism for provisioning. Refer to the Product Setup to access the license server installed in the test subscription for all internal users.

Use one of the following licenses:

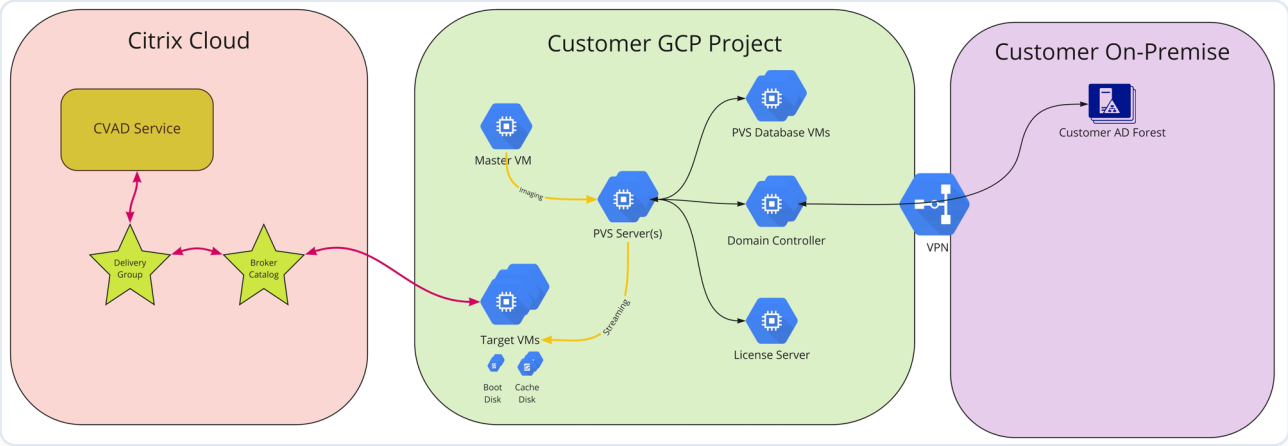
- If you have a Citrix DaaS™ subscription, then use the included **Cloud** provisioning license.
- If you have a Citrix Virtual Apps and Desktops license with Hybrid Rights, then you can use this license directly.
- If you do not have either of these, then contact your Citrix representative to get a suitable trial license.

To install licenses, you can do one of the following:

- Install a license server in your project. This must be on a VM in the project connected to the same VPC and subnet as the provisioning server.
- If there is a VPN connection to your on-premises network, then you can use a license server installed in that network.

Architecture

This high-level architecture diagram shows the components that are either required or recommended to set up Citrix Provisioning on GCP.



This section describes the main components.

Citrix Cloud™

Citrix Cloud has Citrix DaaS instance to integrate with Citrix Provisioning on GCP and includes the following:

- Broker
- Broker Catalogs that include the provisioning target VMs running on GCP.
- MCS HCL plug-in that power manages these GCP VMs.

The Broker starts power management by communicating directly to GCP through the MCS plug-in. As the VM boots, it streams the boot disk from the virtual disk maintained by the Citrix Provisioning server.

Active Directory classic version

Citrix Provisioning on GCP supports only classic Active Directory (AD). There are two ways this can be made available in GCP:

- The GCP Managed Microsoft AD feature can be used to create an AD domain managed by GCP.
- You can create a classic AD domain within your subscription by creating a VM that is configured as a domain controller.

SQL Server

This release supports SQL Server 2019, including SQL Server 2019 Express, installed on a separate server or on one of the Provisioning servers, and Google Cloud SQL for SQL Server.

Supported authentication types

See Supported authentication types for more information on the supported authentication types. Select the authentication type that best suits your needs.

Citrix Provisioning Server

Install the Citrix Provisioning server on a server-class GCP VM, similar to on-premises deployments. This must use a machine size of e2-standard-4 or above and use SSD persistent disk.

You can provide storage for virtual disks as:

- Local storage on the Citrix Provisioning server VM.
- On a separate VM that acts as a file server for sharing vDisks.

Target VMs boot using a small boot disk

The Citrix Provisioning server and target devices do not support PXE or ISO boot, because they are not available on GCP. Instead, target VMs boot use a small boot disk (BDM Boot Disk, which is about 20 MB). This small boot disk contains the Citrix Provisioning UEFI boot application. After the BDM boot application runs, it uses the Citrix Provisioning protocol to stream the virtual disk contents to the VM. Master VMs have their setup modified on the OS disk so that they boot from the provisioning server.

Provisioning of target VMs

The Citrix Virtual Apps and Desktops Setup wizard can handle all the required steps for provisioning target VMs including:

- Creation and upload of the boot disk, including configuration of provisioning servers to make contact.
- Creation of Active Directory computer accounts, or import of existing computer accounts.
- Creation of the target VM, including the network connection, boot disk, and Citrix Provisioning Write-Back Cache (WBC) disk to hold the cache.
- Configuring the provisioned target devices in the provisioning server database.
- Initial start and shutdown of the target VMs to enable the WBC disk to be formatted.
- Creation of a Citrix Virtual Apps and Desktops catalog and adding the provisioned target devices to the catalog.

Citrix Provisioning Master VM

Master VMs are created using normal GCP methods. However, they must be set up to enable UEFI networking, which is not currently possible in the GCP console (see later for details). After this is done, you can use the normal imaging tools to create a virtual disk from the master VM OS Disk (P2PVS and the Imaging wizard).

Set up Citrix Provisioning on GCP

This section explains the preinstallation tasks, steps for creating a Citrix Provisioning collection with a set of target devices streamed from your virtual disk, and links to the GCP documentation to guide you.

To set up GCP provisioning, begin by configuring your provisioning server and other infrastructure on GCP. Using the GCP Console, gcloud CLI, or GCP APIs and the instructions, set up the

components along the same lines as your current on-premises setup. You can create scripts to automate the process.

Preinstallation tasks

Complete the following tasks before installing and configuring Citrix Provisioning.

Establish a virtual private cloud (VPC) and subnets for streaming on GCP

You can use the default VPC that is set up for you or create your own VPC. Provisioning on GCP also supports the use of shared VPCs where Provisioning target devices run in one or more Service Projects sharing the VPC.

(Recommended) Set up IAP Desktop access for secure VM access

For secure external access to VMs running in the subscriptions, we strongly recommend that you create your infrastructure VMs with NO public IP address and configure IAP Desktop to enable secure RDP connections as documented at Configure IAP Desktop.

Select and configure the database

Each Provisioning farm has a single database. You can provide the database on:

- A new or existing SQL Server or SQL Server Express Instance.
- Google Cloud SQL for SQL Server.

All Provisioning servers in a farm must be able to communicate with the database server.

There are three ways to create the database:

- Use the Configuration Wizard. To use this option, you need dbcreator permission.
- If you do not have permission to create databases, use the `DbScript.exe` utility to create a SQL script that a database administrator can run to create the provisioning database. This utility is installed with the provisioning software.
- If the database administrator creates an empty database by running the `DbScript.exe` utility, then this database is chosen as the database for the new farm when running the configuration wizard. The login used when running the Configuration Wizard must be the owner of the database. Also, this login must have the **View any definition** permission. The database administrator sets this permission when the empty database is created.

Run the DbScript.exe utility to create or update the database

See Pre-installation tasks for information on running the `DbScript.exe`.

Configuration wizard user permissions

You must have the system privilege of a local administrator to run the configuration wizard.

For more information, see Configuration wizard user permissions.

Service account permissions

The service account for the Stream and SOAP services must have the following system privileges:

- Run as service
- Registry read access
- Access to `Program Files\Citrix\Citrix Provisioning`
- Read and write access to any virtual disk location.

For more information, see Service account permissions.

Set up Active Directory

Use one of the following methods to support Active Directory APIs and functionality on GCP:

- Enable the GCP Managed AD service in your project by following the instructions at Running Active Directory on Google Cloud.
- Create Active Directory domain controller VMs in your subscription and connect to an on-premises forest through a VPN connection if necessary.

Create a connector VM on GCP

Create VMs to act as cloud connectors in each unique combination of region and project you are using. Then, install a Citrix Virtual Apps and Desktops Cloud Connector in it. Once this is done, add hosting resources to your Citrix DaaS referencing the resource locations.

Create a Citrix License Server

Do one of the following:

- install the License Server on one of the Provisioning servers.
- create a dedicated VM or configure a connection to an existing on-premises License Server.

Create the Citrix Provisioning Server on GCP

Create VMs for the Provisioning servers. Size servers for the expected load, similar to on-premises Provisioning servers.

The Citrix Provisioning server VMs require the following resources:

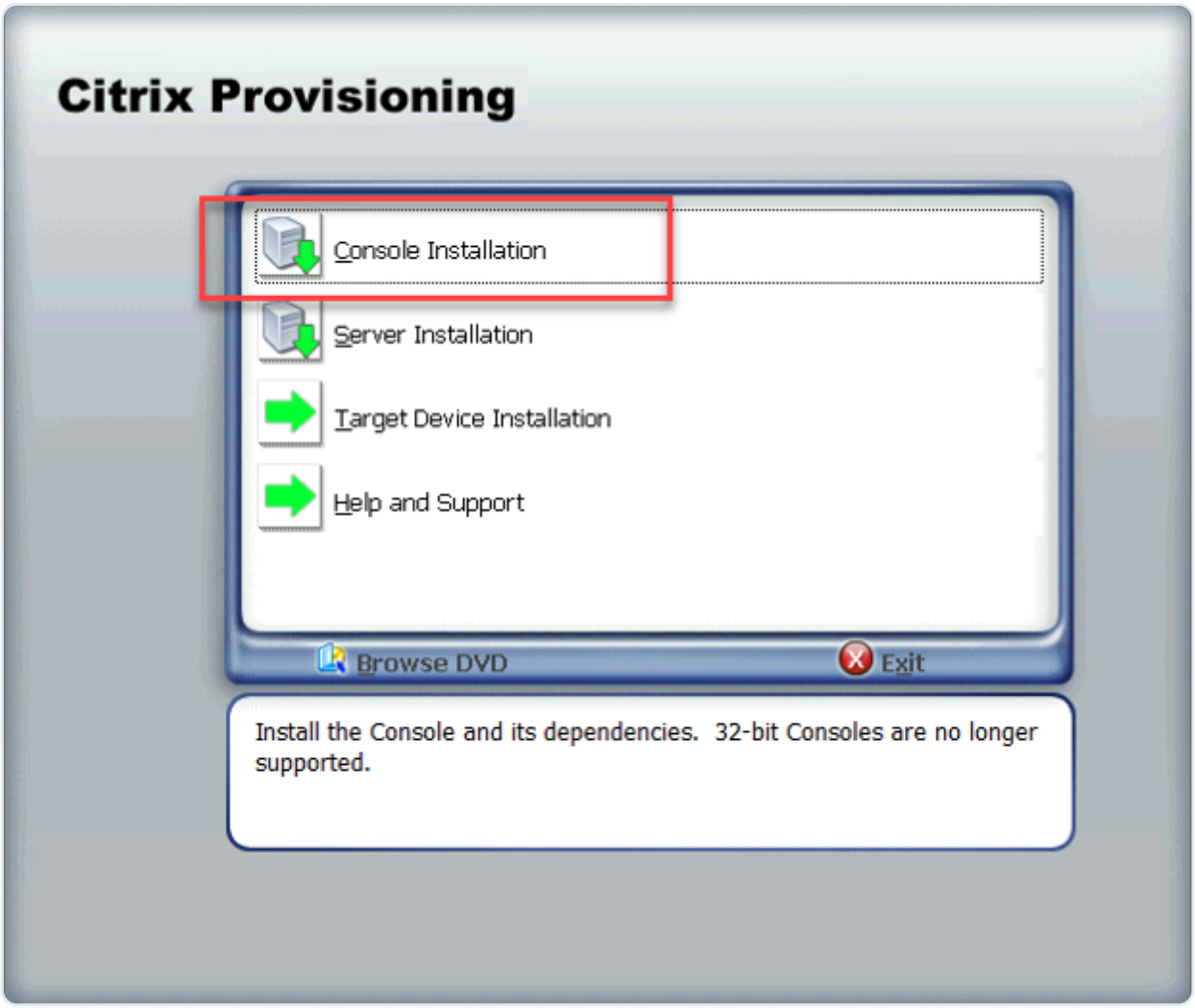
- Access to the SQL database previously configured.
- Access to a license server VM on GCP.
- The Active Directory requirements are the same as for the existing on-premises version of Citrix Provisioning.
- Use of VPC and subnets previously set up to support the installation. As stated above, we strongly recommend NO public IP addresses, and access only using the IAP Desktop Service.
- At least one NIC per server VM, on the same subnet that target devices handled by the server use.
- Access to virtual disk storage. You can use:
  - Local storage on the Provisioning server VM.
  - On a file share implemented by the Google Netapp Cloud Volumes service.
  - On a separate VM providing a file share.
- Minimum of 2 vCPUs, 8 GB RAM each for the Citrix Provisioning server VM. The Provisioning server VMs must have machine size e2-standard-4 or above and use SSD persistent disk.

> **Note:**
>
> In GCP, the number of virtual CPUs assigned to the VM as specified at About Machine Families controls the available network bandwidth for a VM.

Install the Citrix Provisioning software

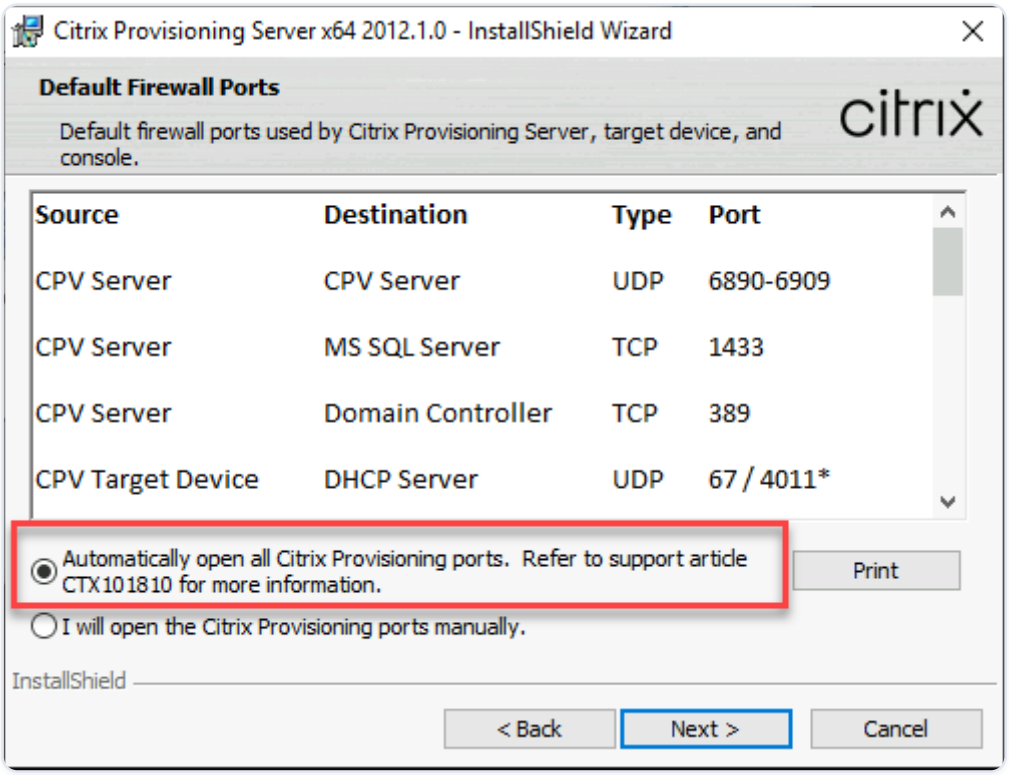
To install the Citrix Provisioning server and console:

1. Using an administrator account, log into the Citrix Provisioning server VM.
2. In File Explorer, select the ISO file, right click, and mount it.
3. In the mounted drive's root folder, find the **autorun.exe** file, and run it. The Citrix Provisioning Installer starts.
4. Start by installing the Console. The installer prompts you to install prerequisites.



> **Note:**
>
> If prompted, reboot, mount the Citrix Provisioning ISO again, and restart the process.

5. Install the Citrix Provisioning server using the **Server Installation** link on the autorun program. By default, creating firewall rules for provisioning traffic is enabled.



Note:

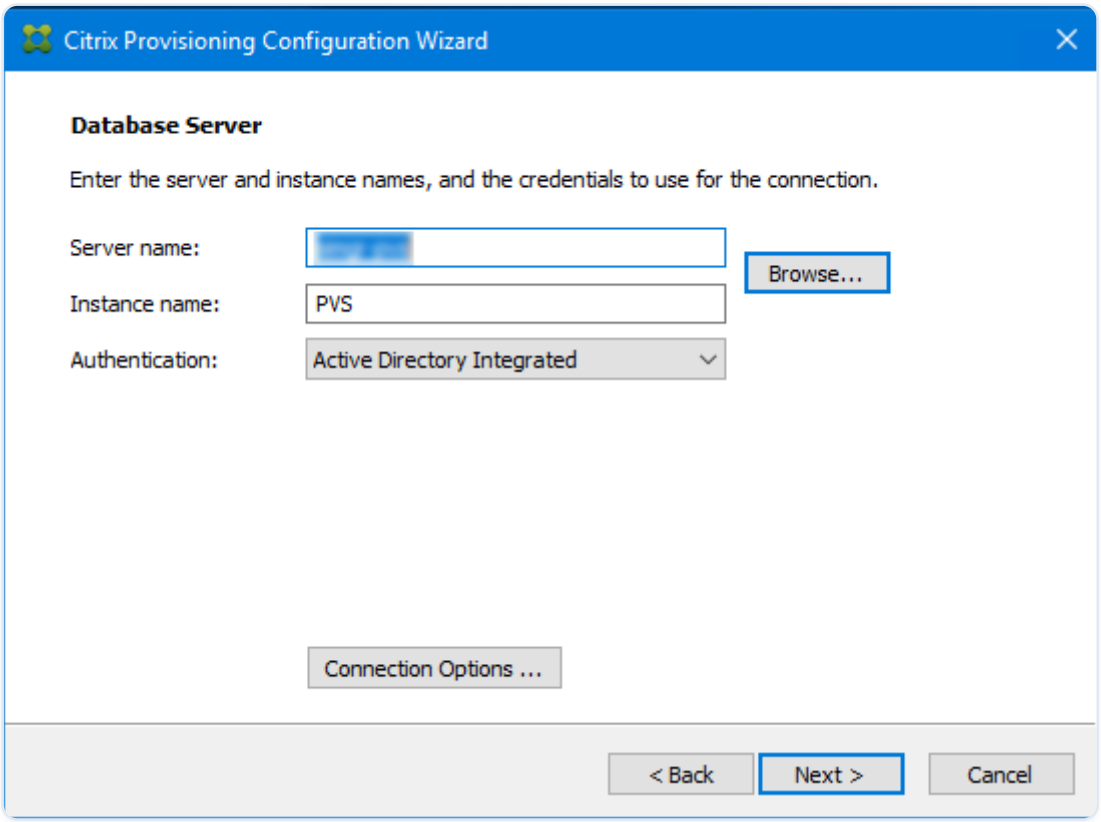
This process sets up the firewall running inside Windows. Any required firewall setup for the VPC must be done outside of this and must allow Citrix Provisioning traffic to flow. See Communication Ports Used by Citrix Technologies for information on ports that must be opened to ensure communication flow.

When the server installation completes, it runs the Citrix Provisioning Configuration Wizard where you set up the provisioning server.

a. Welcome: Read the Welcome dialog and click **Next**.

b. Farm configuration: Indicate whether a new farm is being created.

c. Database server: Enter the SQL Server host name or address and the name of the instance that you created for the Provisioning server to use, or enter the private FQDN of the Google Cloud SQL for SQL Server (leave instance blank). The Authentication drop-down lists the supported authentication types for the Provisioning Service Account to use when connecting to the database. Depending on the authentication mode that is selected, you can provide the necessary credentials for the Provisioning Service Account to connect to the database.



d. When you click next, enter the database administrator credentials that are used by the configuration wizard. Select **Active Directory Integrated** authentication if you want to use the current login.

e. New Farm: Enter the farm, site, and collection names. We recommend selecting Use Active Directory groups for security, and the Farm Administrator group.

f. New Store: Specify the store and location. If you are using a file share, then enter a UNC name.

g. License server: Enter the license server location.

h. User Account: Specify the user account to run the services under. If you use a network share for the store, use a domain account with access to the share. The account must be an administrator on the Provisioning server.

i. Network Communication: Choose the network interface to be used for streaming and management. If you only have a single NIC, accept the defaults.

j. Soap SSL Configuration: Accept the default values.

k. Problem Report Configuration: Enter your MyCitrix credentials to enable submission of cases.

l. Finish: Review the configuration settings, and click **Finish**. A dialog reports a warning about the Windows Firewall.

m. Click **OK**. A progress dialog opens to display progress as Citrix Provisioning is being configured. If failures occur, you receive a link to review the log.

n. When configuration is successful, click **Done**.

Workflow for running the configuration wizard silently

See Running the configuration wizard silently for information on running the configuration wizard silently.

Create the master VM

This section explains how to create the master VM, and prepare the image to connect to the Citrix Provisioning server at start time.

> **Note:**
>
> Be sure to use a Windows Server image from the GCP marketplace. Bring your own images are not supported currently.

> To create the master VM:

1. Create a virtual machine with UEFI Networking enabled:

   a. Use the gcloud CLI or the GCP console.

      - If you use the gcloud CLI, specify the option `--enable-uefi-networking`.
      - If you use the GCP console, you cannot specify that UEFI networking must be enabled and this cannot be changed after the VM is created. We have provided a script `Update-PVSMaster.ps1` that can be used to recreate a master VM with this flag set. However, this loses any IP configuration associated with the VM.

   b. Set these values:

      - Networking interfaces to select the subnet setup for streaming.
      - Specify no public IP address.

   c. Log in to the VM using IAP Desktop and complete the Windows setup. Select the option to create a new administrator account initially.

   d. Join the domain used by your Citrix Provisioning deployments.

e. Deploy the VDA, using standard practices.

2. Ensure that the VM is configured to allow networking at UEFI start time. If you have a VM that does not have this flag set, run the `Update-PVSMaster.ps1` script to convert it.
3. Install the Citrix Provisioning target device software.
   a. Mount the Citrix Provisioning ISO.
   b. Select to install the target drivers.
   c. Restart when prompted.
4. Run the imaging wizard, as you would do for an on-premises installation.
   a. Specify the **Server name or IP address**, and select **Use my Windows credentials**.
   b. Imaging Options: Select **Create a vDisk**.
   c. Add Target Device: Specify the **Target device name** and the **Collection name**.

> **Important:**
>
> Use a different name than the current host name. The master VM can boot either from the local disk or from the virtual disk you create, but computer account password management is not synchronized between them. If you give the target the same name as the current host, you lose domain trust when switching between the two ways of starting the master VM.

   d. New vDisk: Specify the virtual disk name.
   e. Microsoft Volume Licensing: Select **KMS Licensing**.
   f. What to Image: Select **Image entire boot disk**.
   g. Optimize Hard Disk for Citrix Provisioning: Select **Optimize the hard disk** to ensure that unnecessary Windows features are disabled.
   h. Summary: Verify that the settings are correct. Click **Create** when prompted. Restart the VM.
   i. When the Master VM finishes booting, log on again. The imaging wizard resumes where it is left. Select **Cancel** when a dialog displays to format the disk.

> **Note:**

> The imaging takes some time.

j. When imaging is complete, exit the imaging wizard.

k. On the Citrix Provisioning Console:

- Update the vDisk to Production status, with **Cache Type** set to **Cache in device RAM with overflow on hard disk**.
- Right-click the master VM target definition, and select **Active Directory > Create Computer Account**.

Create target VMs using the Citrix Virtual Apps and Desktops Setup wizard

The Citrix Virtual Apps and Desktops Setup wizard lets you create multiple target VMs in a single invocation. The wizard guides you through the complete process of creating target VMs and integrating them with Citrix Virtual Apps and Desktops and Citrix DaaS.

Initial Setup

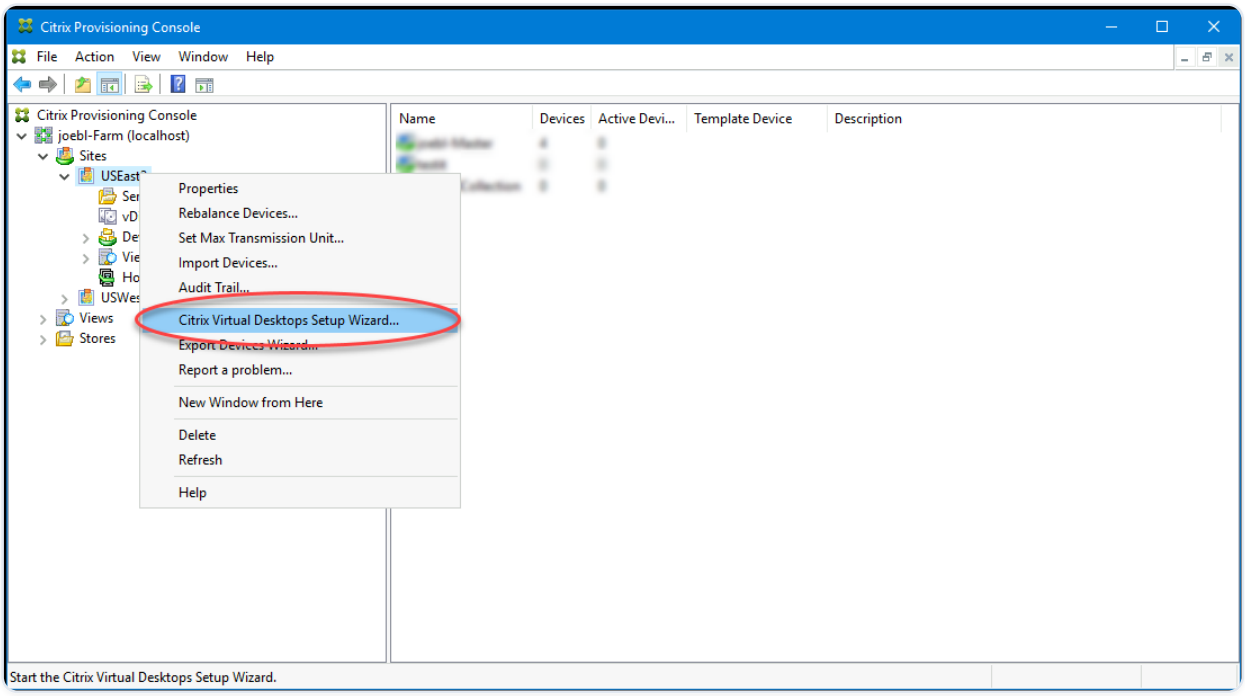
Do the following once before running the Citrix Virtual Apps and Desktops Setup wizard:

1. If you want to use your own Service Key for accessing GCP, follow the guidance in Creating and managing service account keys to create and download a Service Key. If you plan on using the same service key that was created for use by Citrix DaaS, then use Service Key JSON file.

Create target VMs

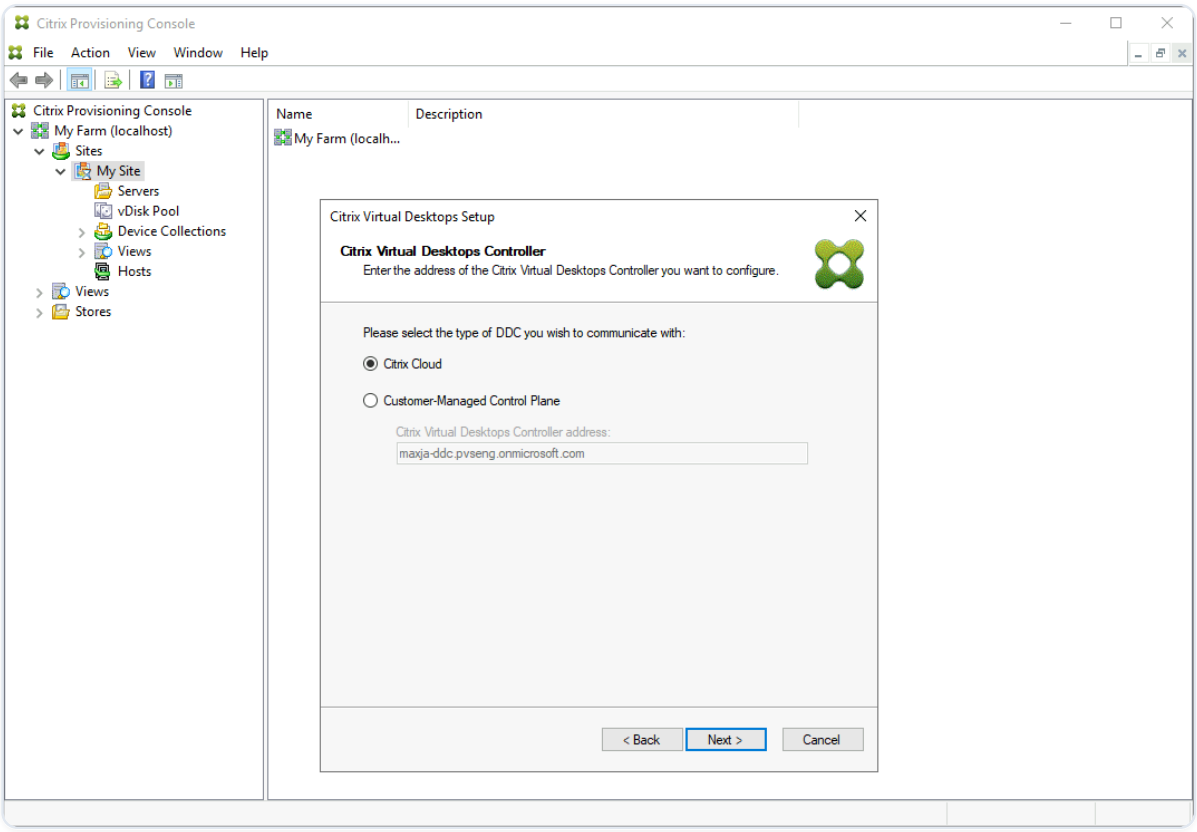
To create target VMs using the Citrix Virtual Apps and Desktops Setup wizard:

1. Run the provisioning console, right-click the site where you want to create target devices, and select **Citrix Virtual Desktops™ Setup Wizard**.

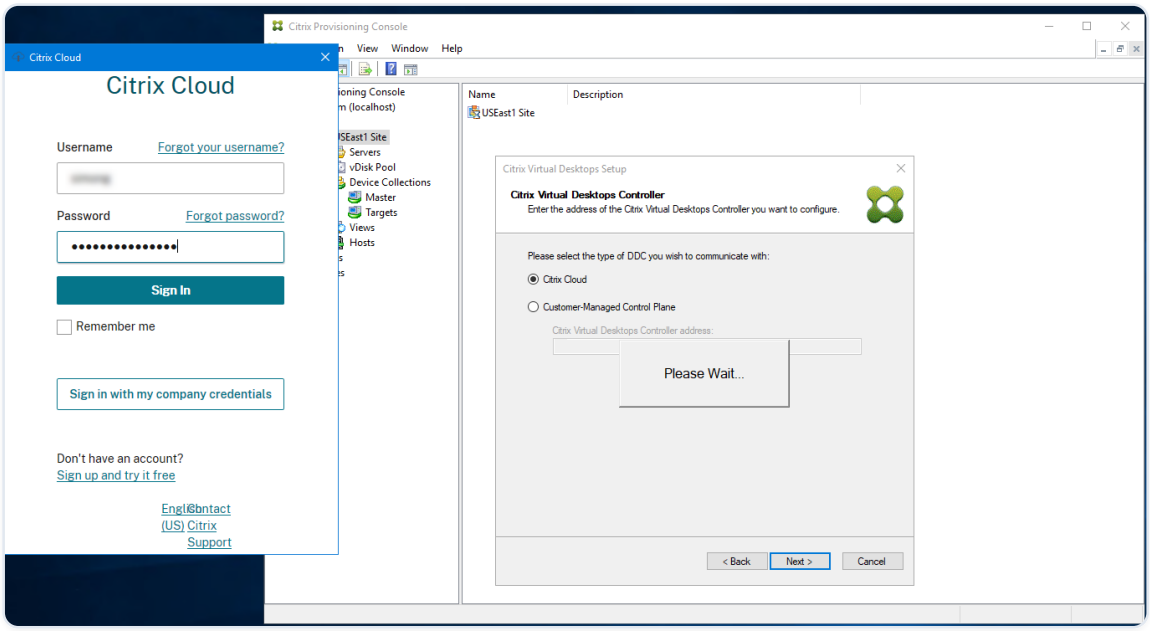


2. Click through the welcome page, select the type of Delivery Controller, and choose **Next**.

   a. If you select **Citrix Cloud**:



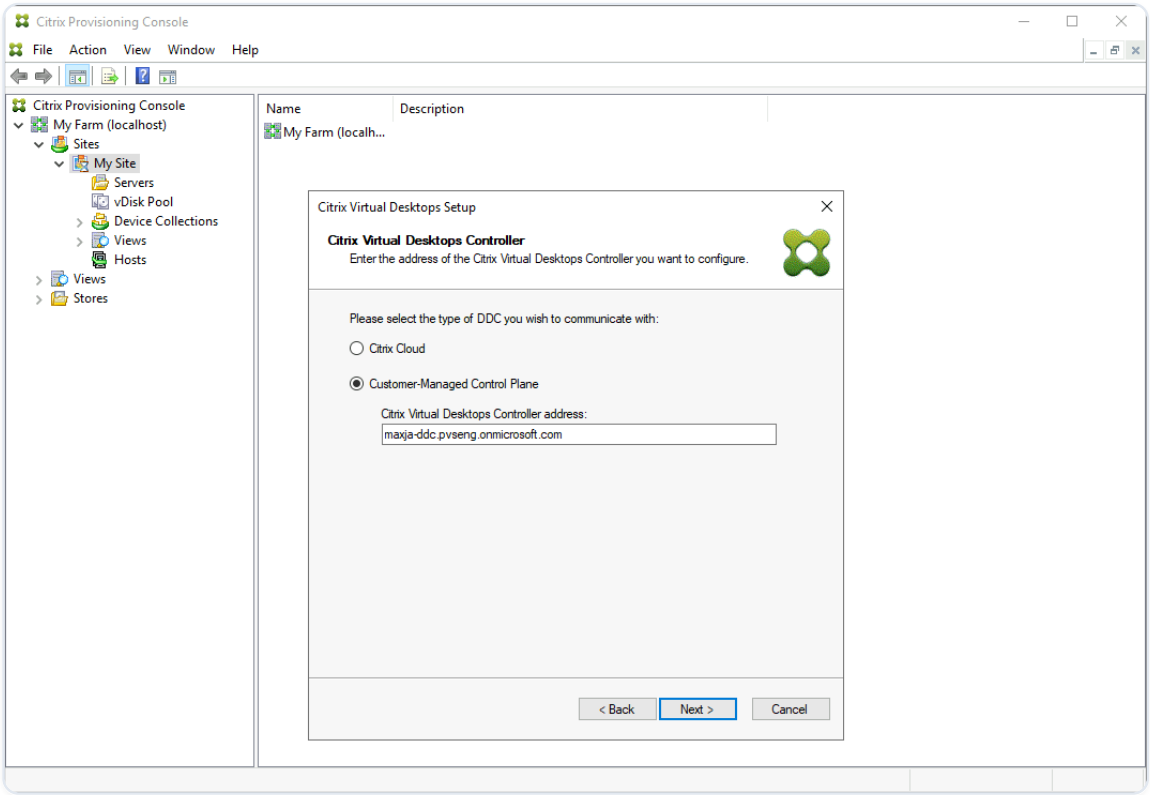
   i. Enter Citrix Cloud credentials when prompted.



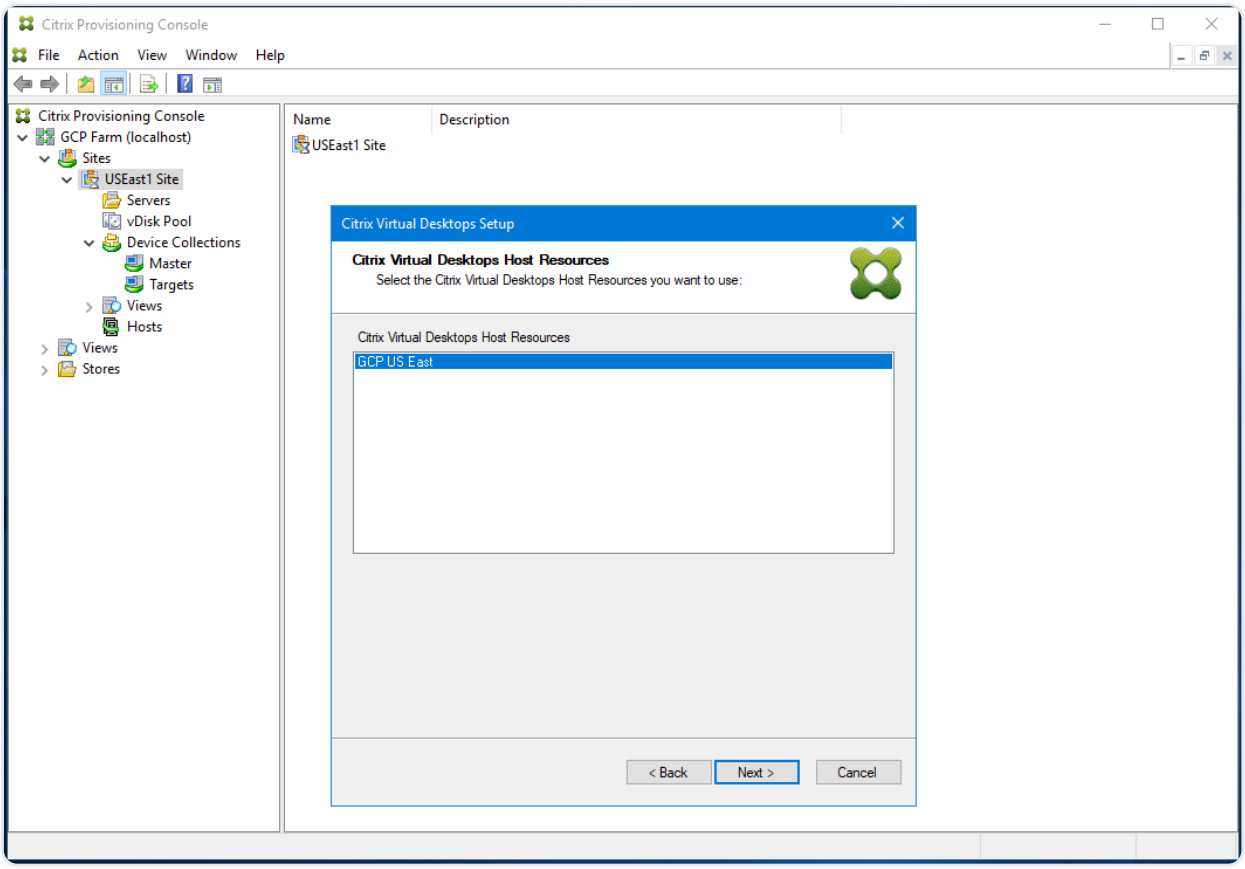
ii. If you have more than one customer, select appropriate cloud customers.

b. If you select **Customer-Managed Control Plane**:

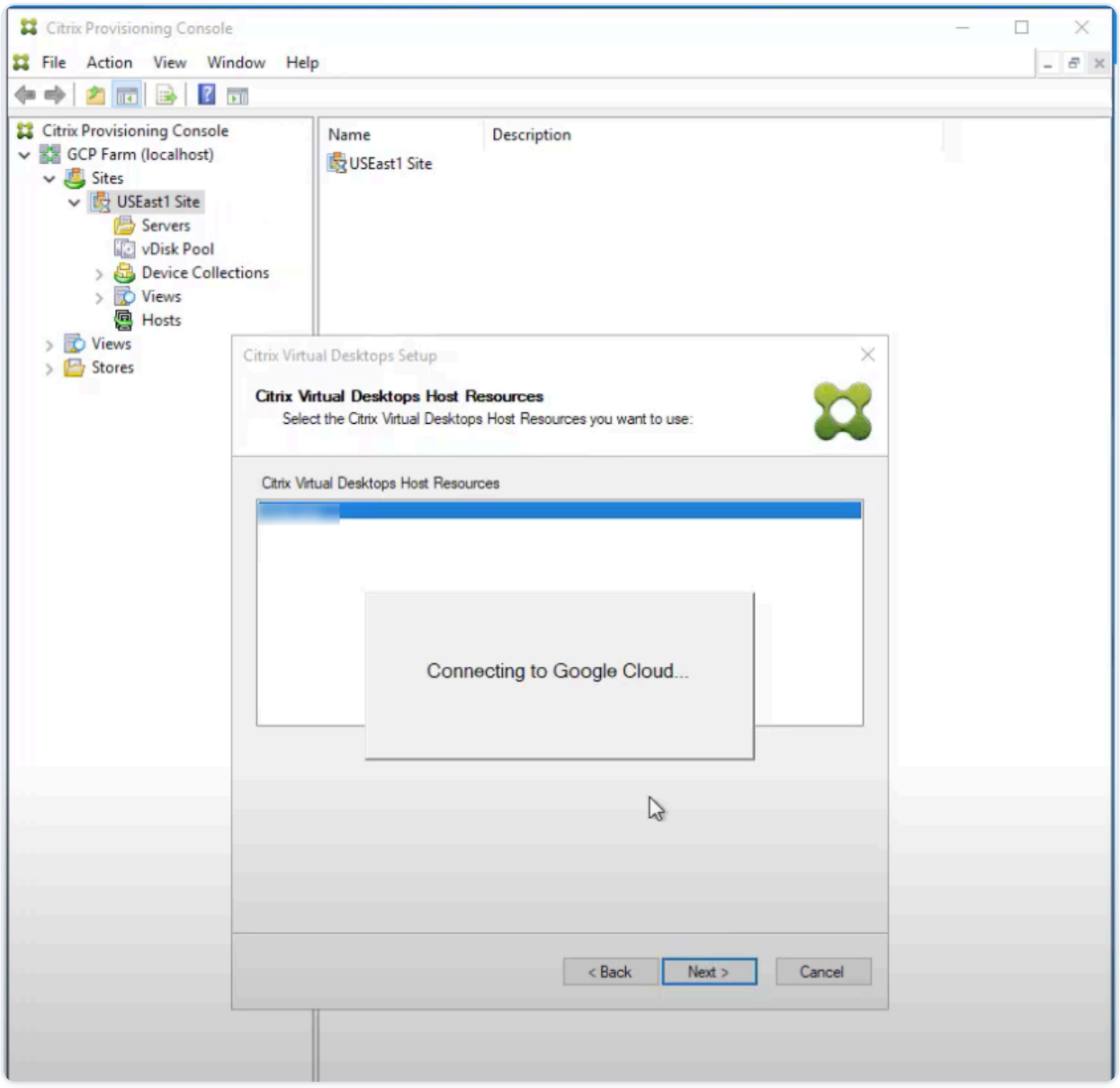
i. Enter the controller hostname or address. The wizard authenticates to the Delivery Controller using the current logged in user.



3. Choose a GCP hosting unit from the displayed list. The wizard displays the list that it retrieves them from the Cloud. Select the hosting unit to use based on the region and project you are provisioning to.



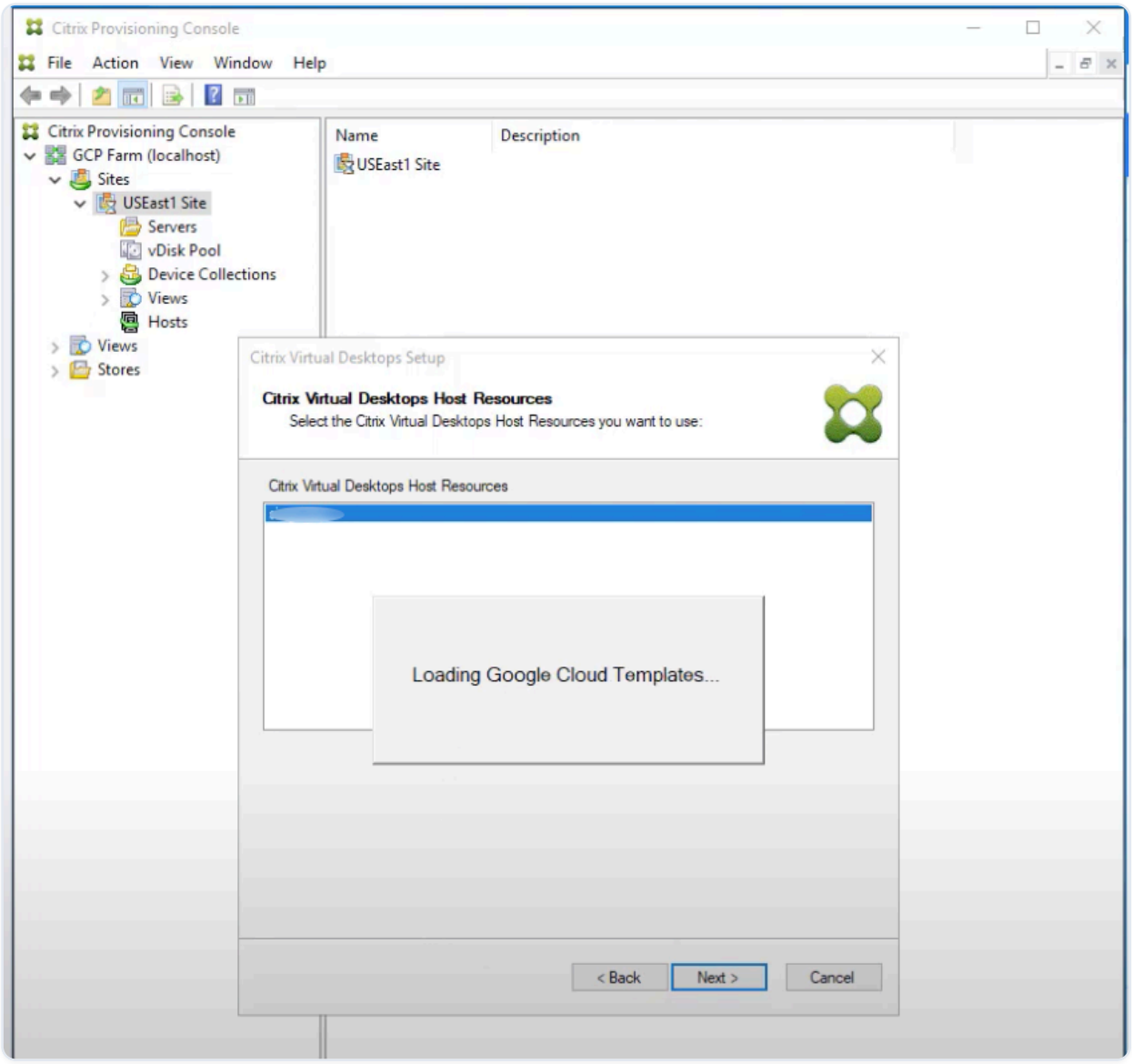
4. After you select the GCP hosting unit in Hosting Resources screen, and click **Next**. You receive a message **Connecting to Google Cloud…**. A new web browser opens up. Enter your google credentials to log in to your google cloud.



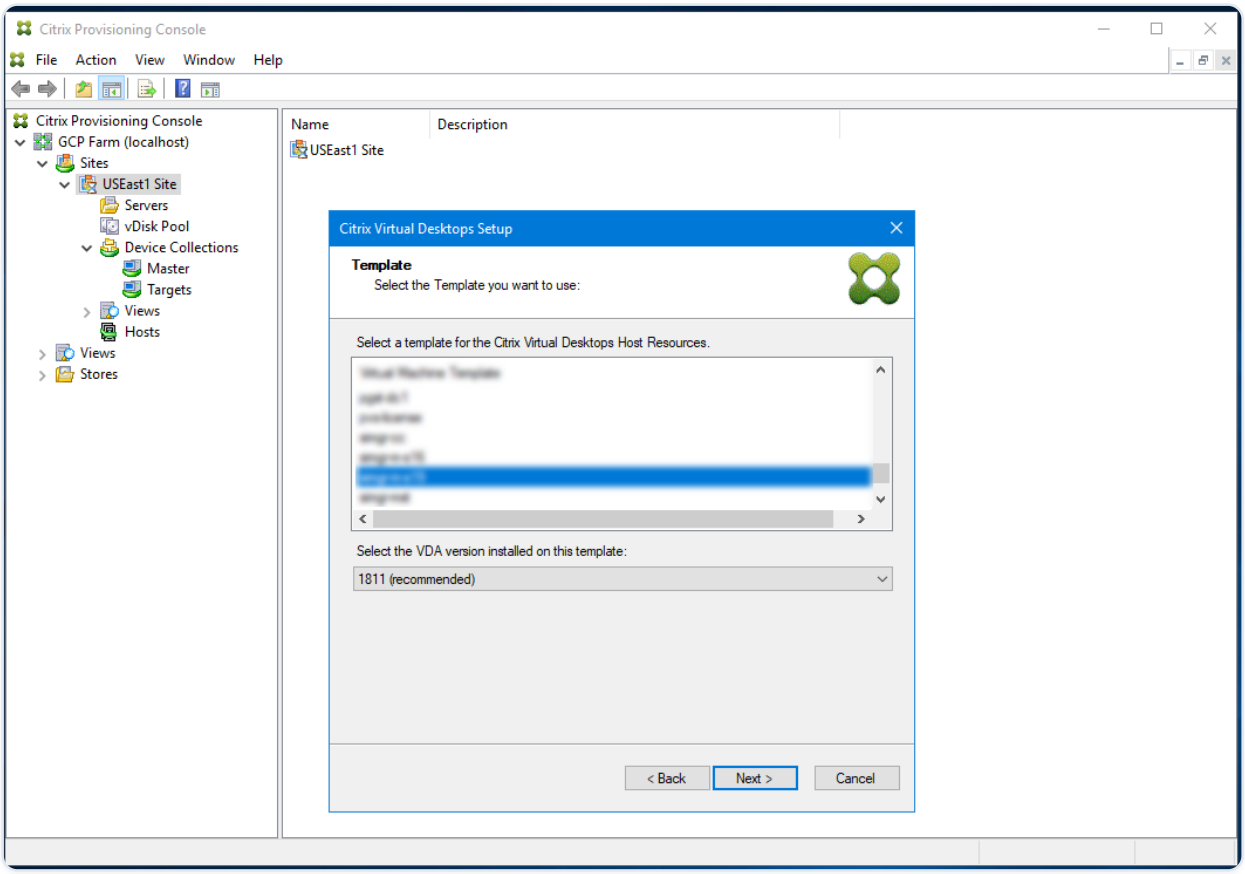
Note:

If you previously logged in to the google cloud and approved the permission for the app, the browser to enter your google credentials does not appear.

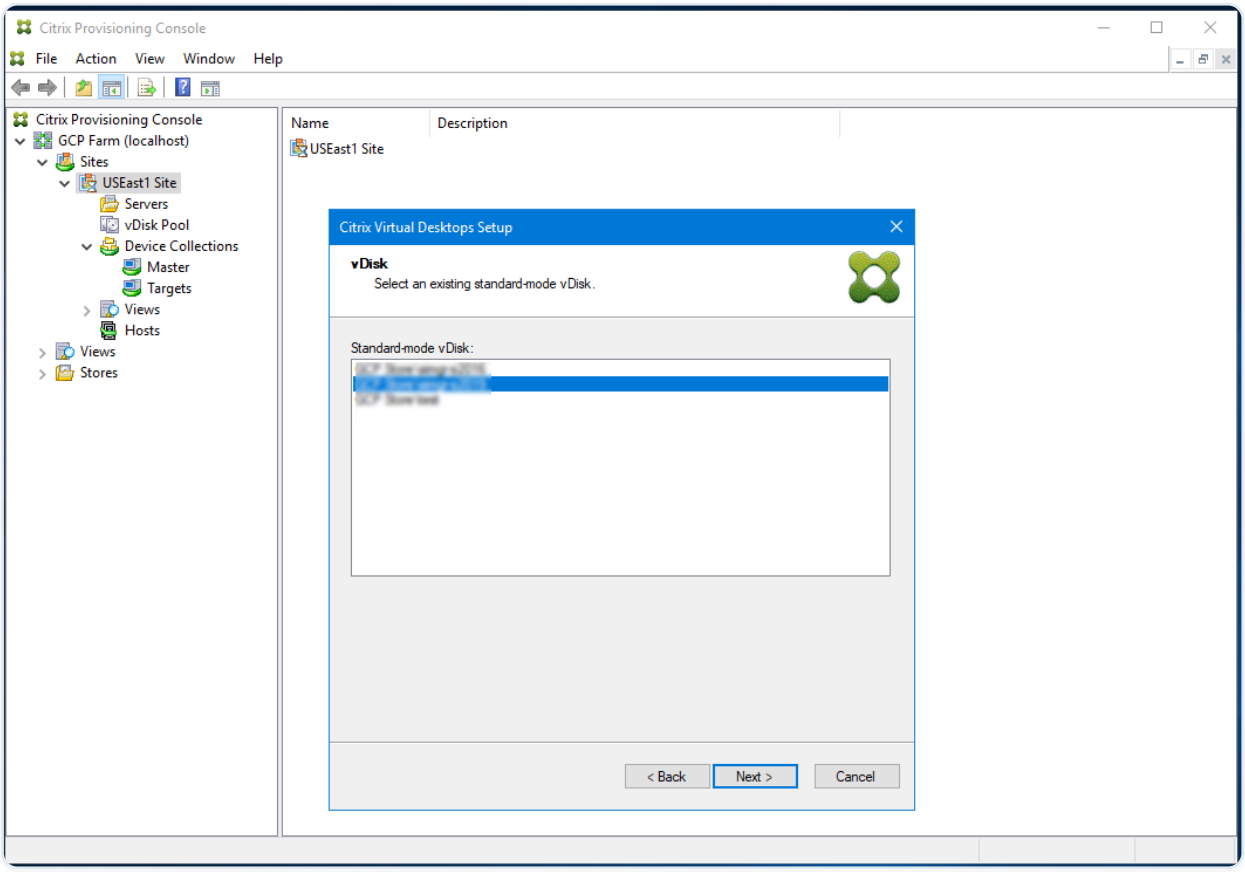
5. After a successful login, you receive a message **Loading Google Cloud Templates..**



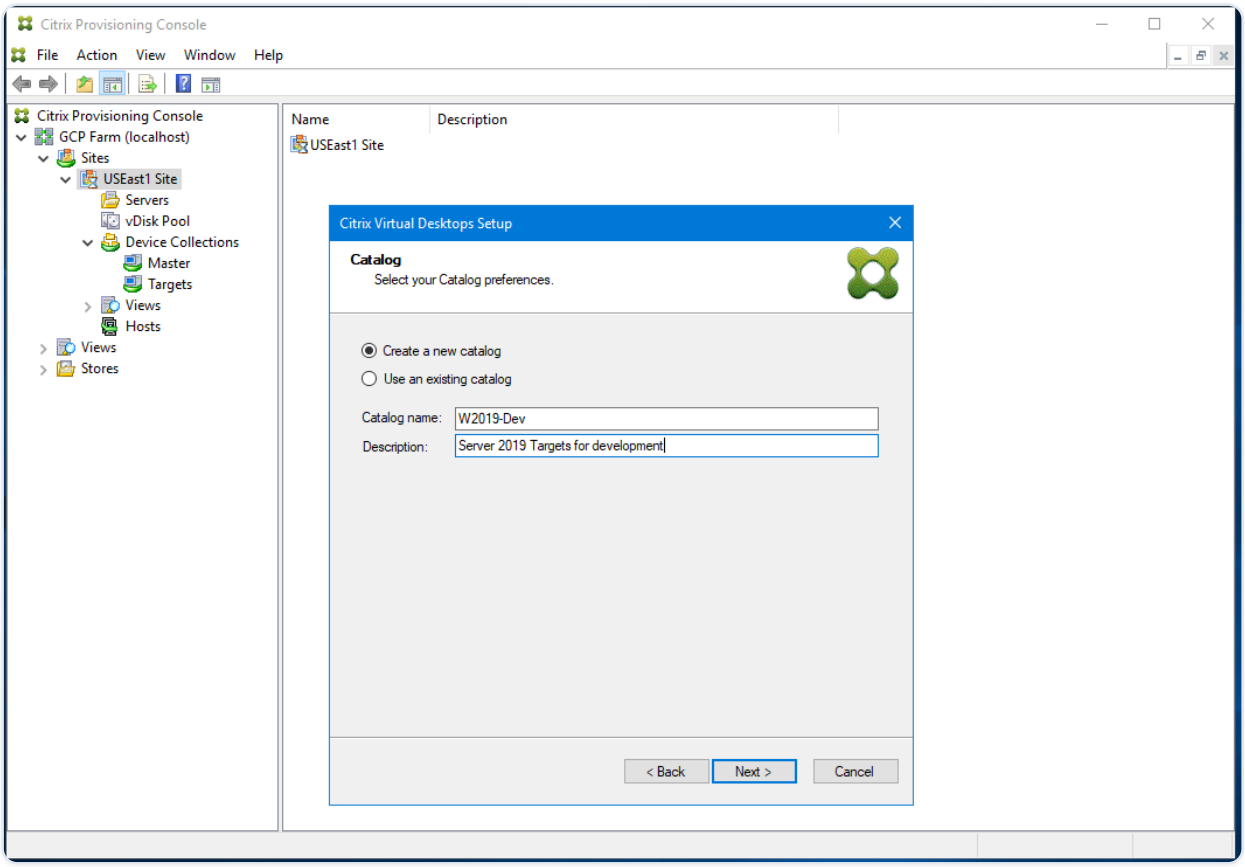
6. Select a VM that can be used as a template for creating provisioned VMs in GCP. Choose the same VDA version that you use for on-premises Citrix Provisioning and MCS. Click **Next**.



7. Choose the vDisk to use for the provisioned target devices.

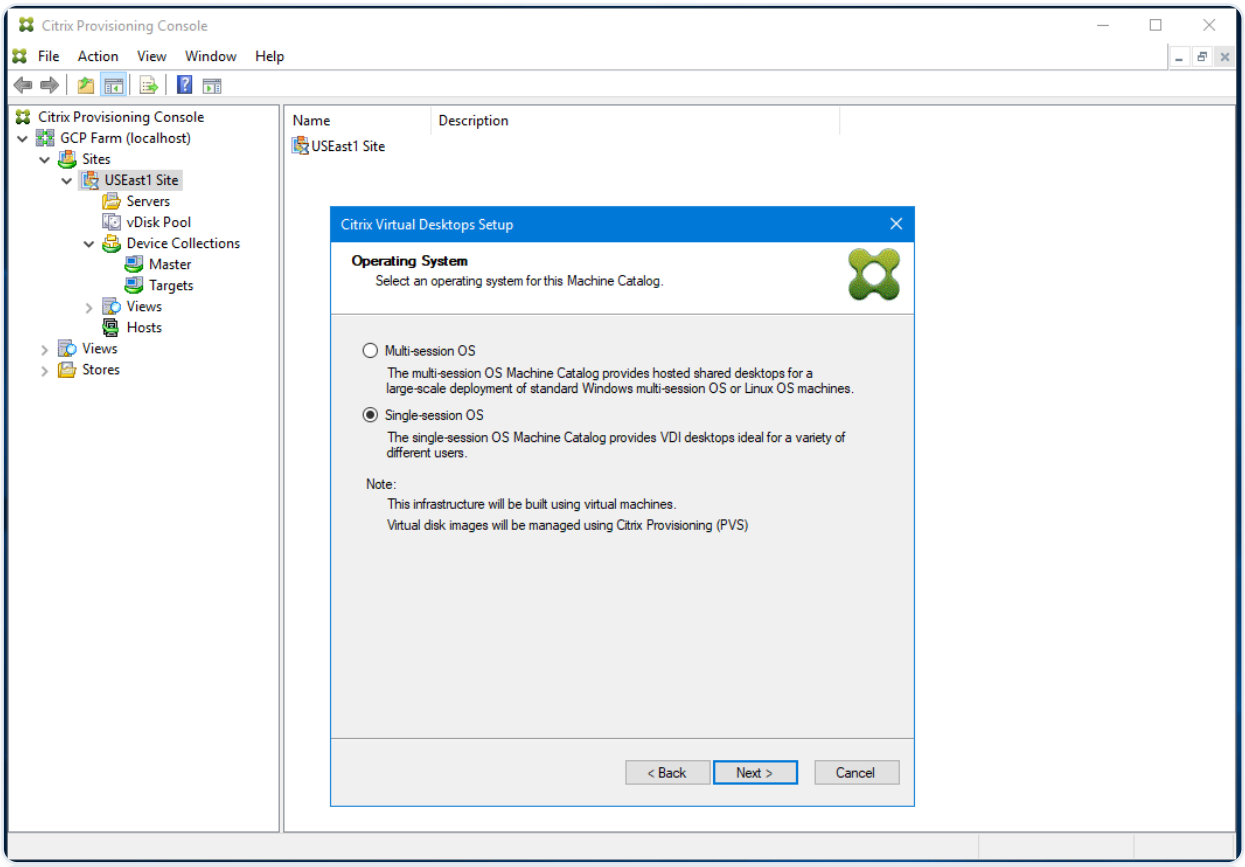


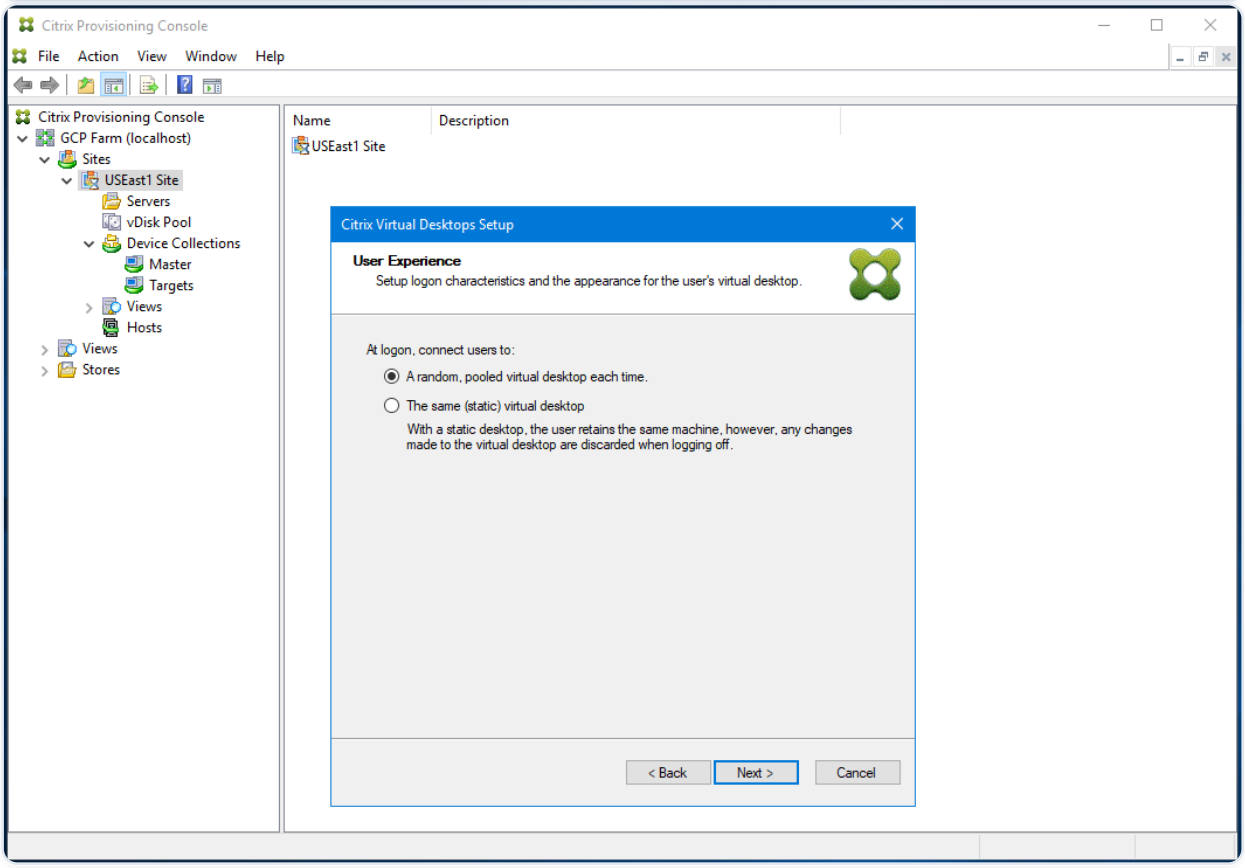
8. Choose to create a catalog, or add the VMs to an existing catalog.



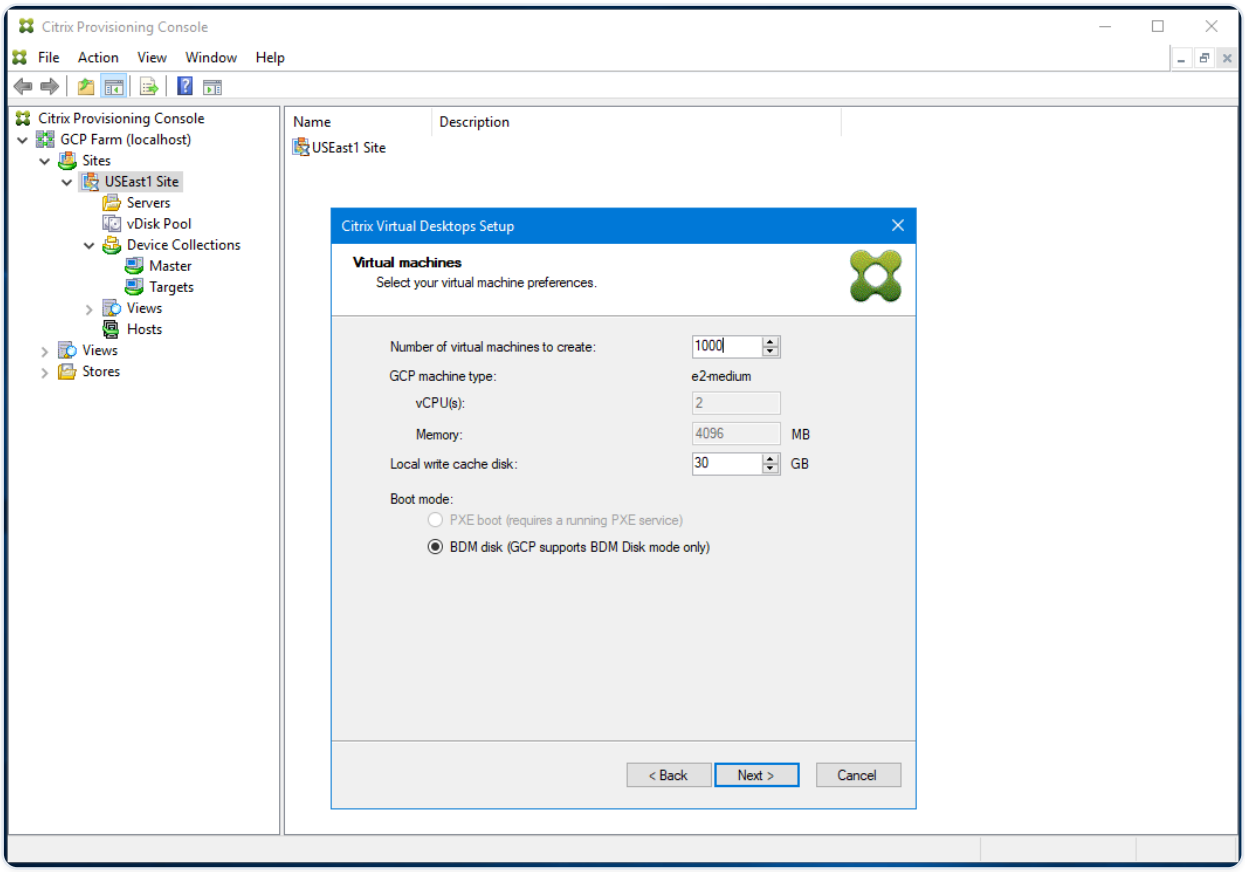
If you add to an existing catalog, a drop-down list of catalogs is supplied for you to choose from.

9. Choose the type of VDA and catalog:





10. Choose the number of VMs to create and the size of the local cache disk. The machine size from the template VM, the number of vCPUs, and memory size are displayed for your information.



> **Note:**
>
> BDM Mode is the only supported boot mode on GCP.

11. Select Active Directory for the target devices.

    Citrix Provisioning supports provisioning of target devices in untrusted domains.

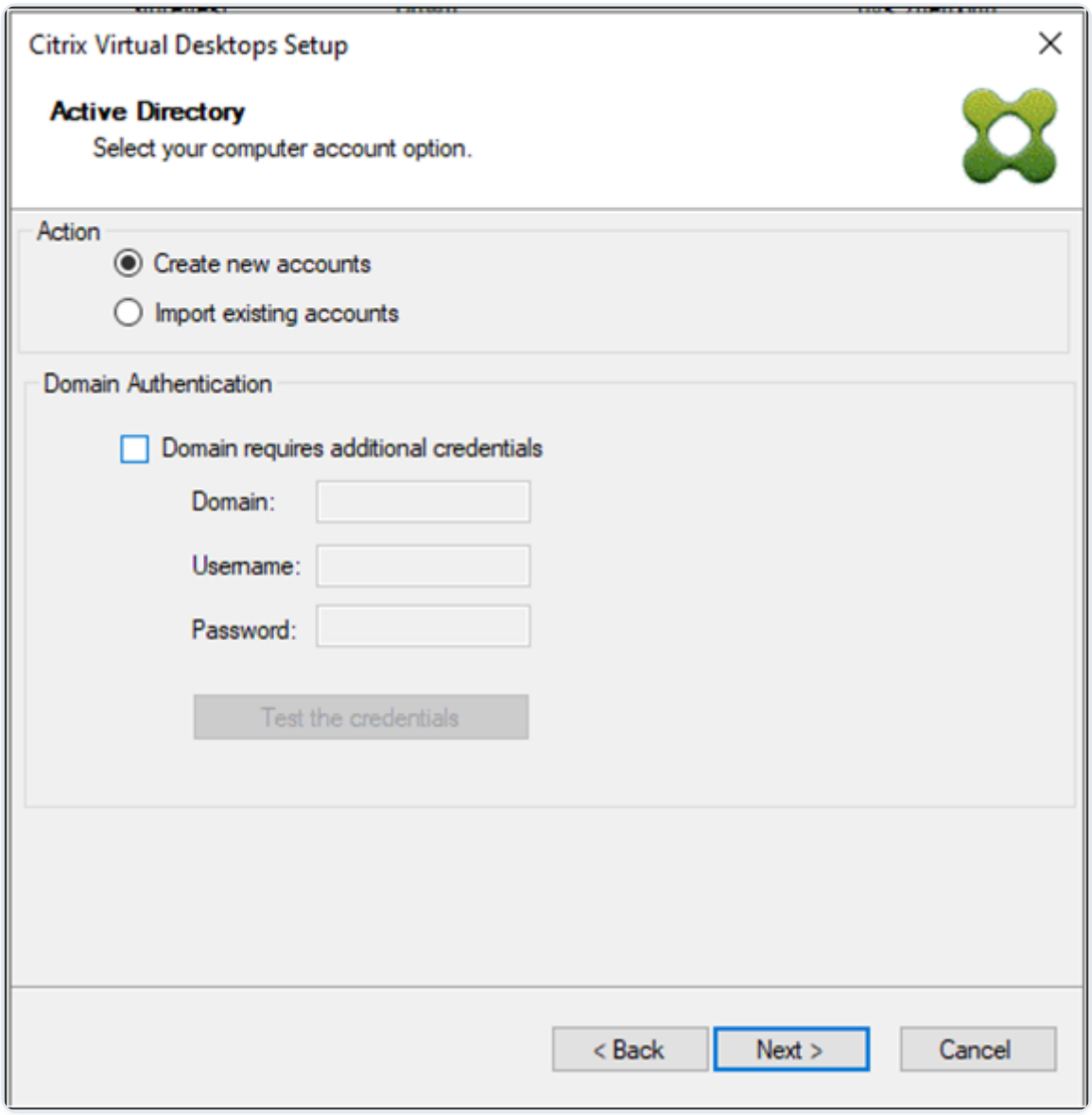
    If the domain is not trusted, under **Domain Authentication**, do the following:

    a. Select **Domain requires additional credentials**.

    b. Enter the domain name, username, and password for the untrusted domain.

    c. Click **Test the credentials**. This action validates the domain name and the credentials.

    d. After you get a green check mark, proceed to the next page.



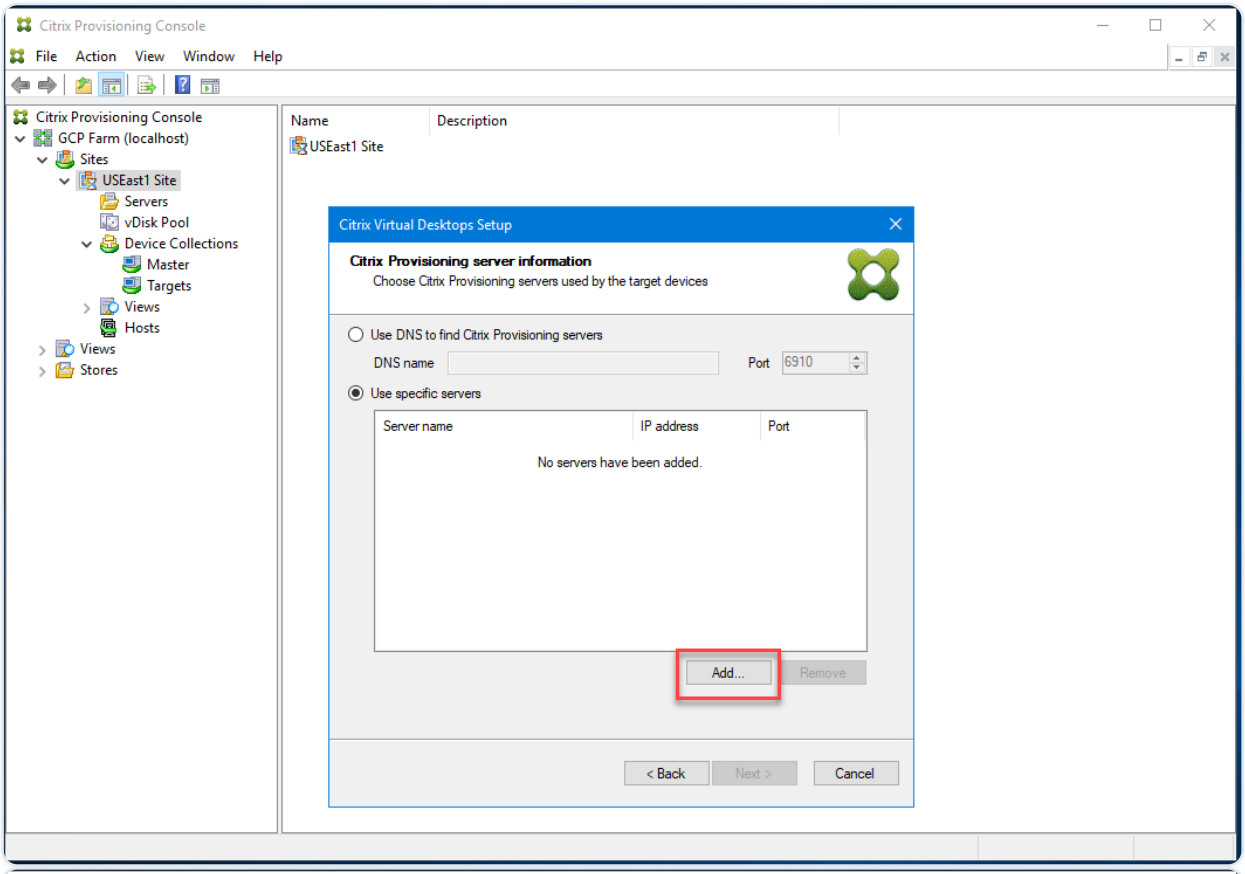
Note:

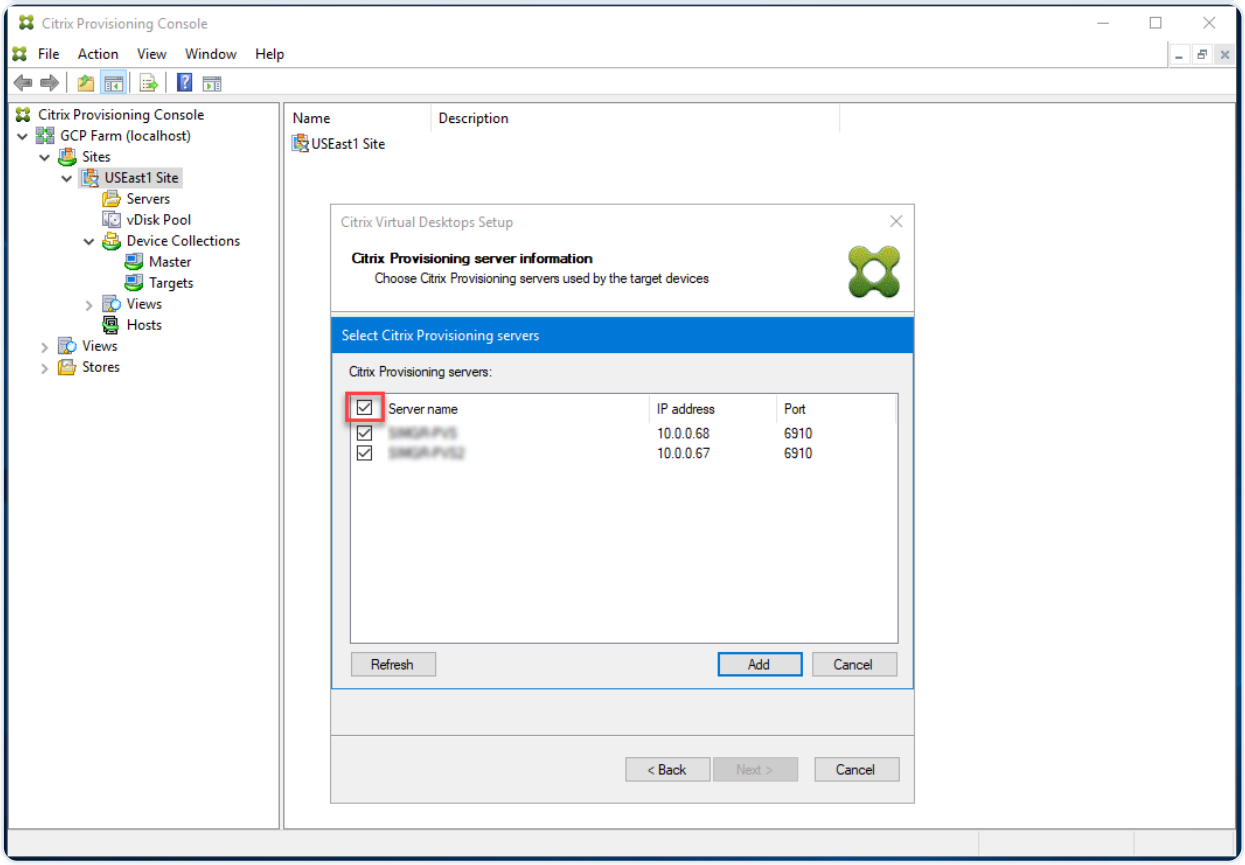
You must only include lower case letter, numbers, or hyphens in the naming scheme as this name is also used for the name of the VM that is created. Other letters (including uppercase letters) are not allowed.

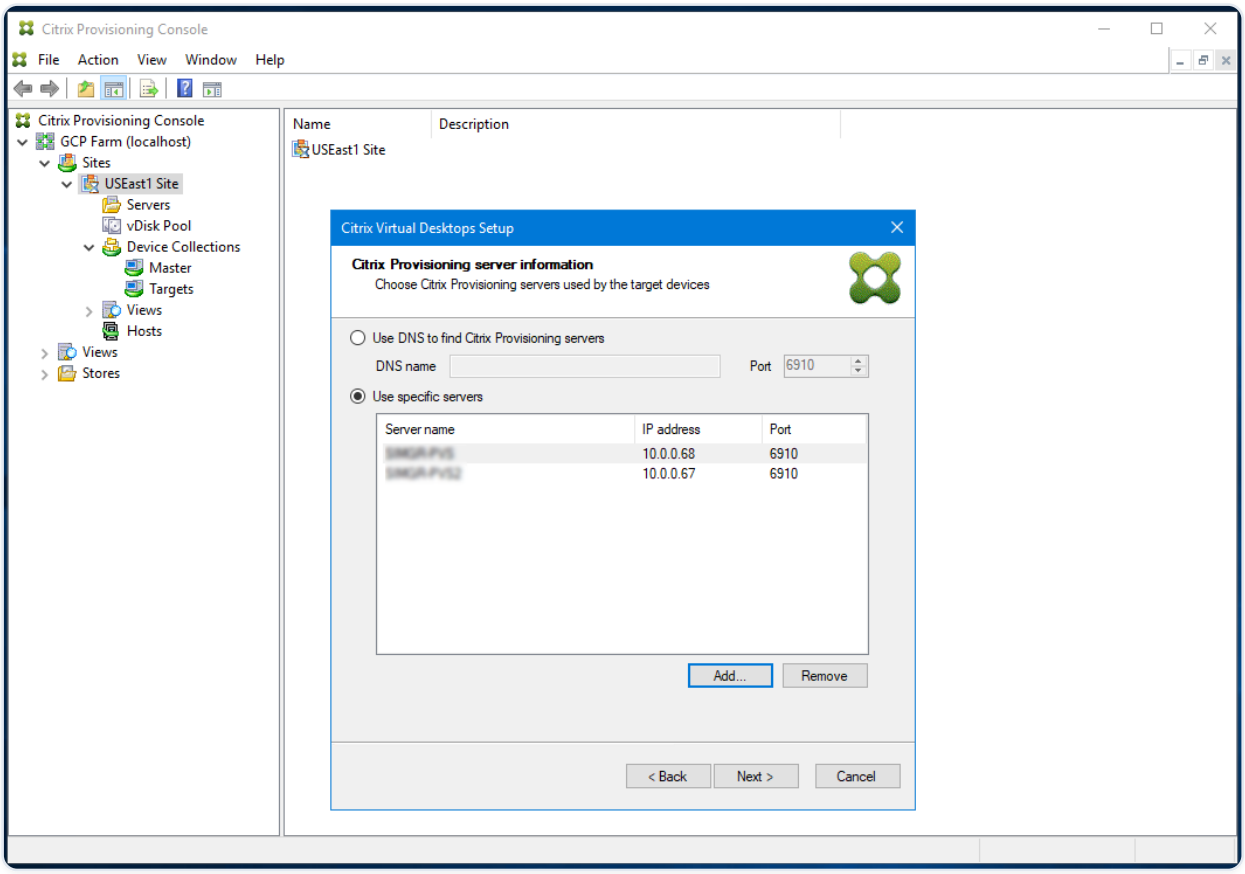
In addition, if using a GCP Managed AD instance, you must create computer accounts underneath the `Cloud` OU.

12. Set up the information about the provisioning servers that function as login servers for the target devices.

As with the on-premises product, you can use either a DNS FQDN that translates to a set of servers, or you can specify the desired servers by IP address. If you use an IP address, click **Add** to display the list of configured servers:



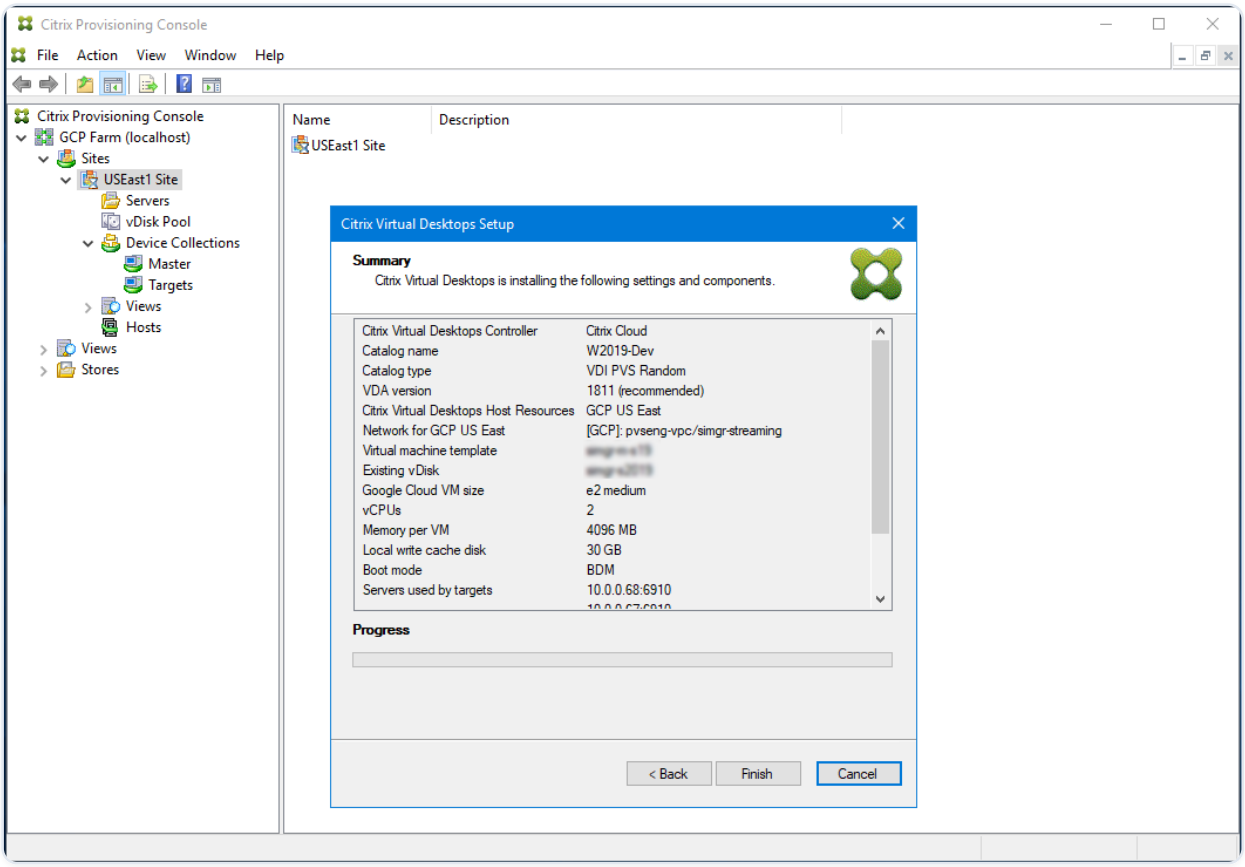




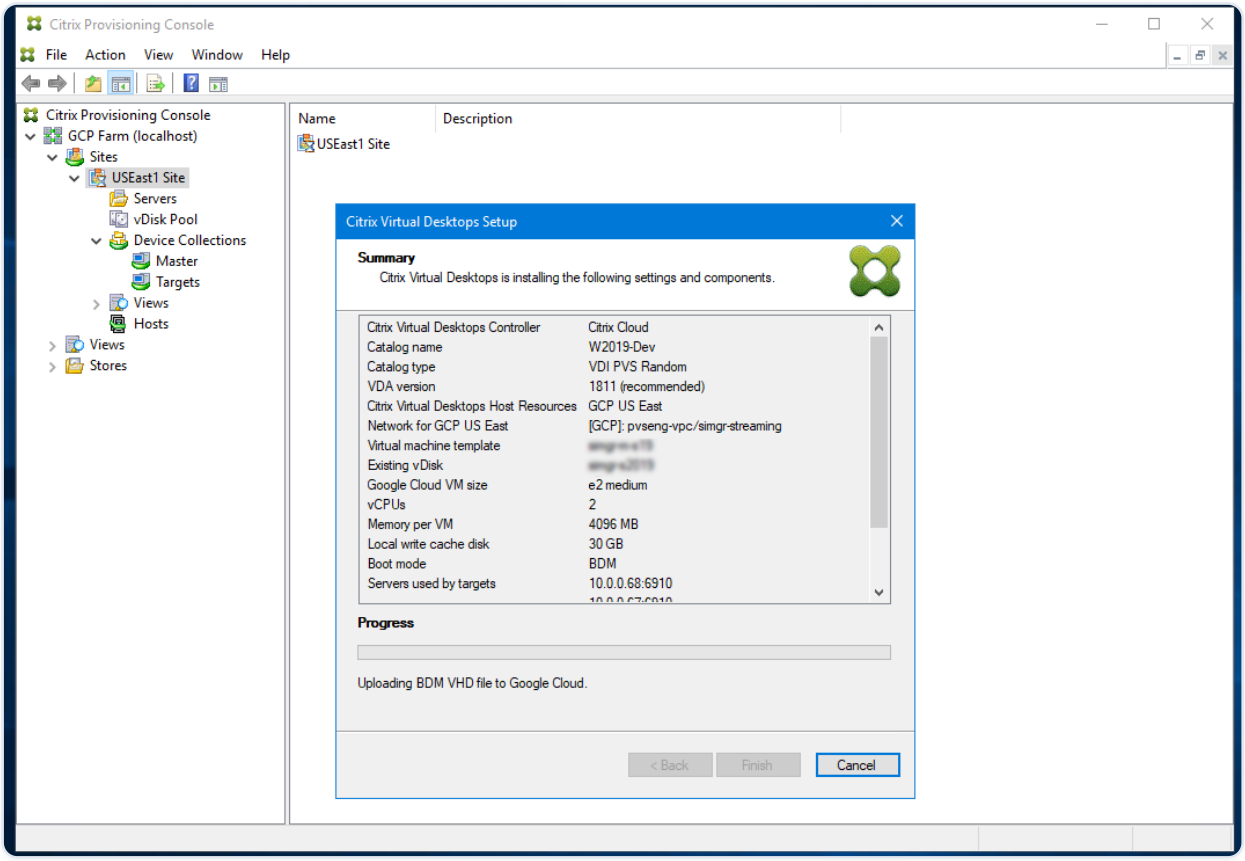
Note:

If you want to use a DNS name, then you must specify the fully qualified domain name as the default DNS suffix supplied by the GCP. DHCP server does not include the zone where you add the DNS name to be used.

13. Verify the information on the summary page, and click **Finish** to begin the provisioning process.



As the provisioning operation is proceeding, the progress bar at the bottom is updated.



Also, consider the following:

- During the Citrix Virtual Apps and Desktops Wizard process, the newly created VM boots up to format the write cache disk, then shuts down. This process takes a few minutes. If the machine times out during this operation, the setup process fails.

Manually creating target VMs on GCP

Citrix recommends using the Citrix Virtual Desktops Setup wizard to create target VMs and integrate with Citrix Virtual Apps and Desktops and Citrix DaaS, as documented in the previous section. If you cannot use the Citrix Virtual Desktops Setup wizard, then you can manually provision target VMs using the procedures outlined in this section.

The Citrix Provisioning server and target devices do not support either PXE or ISO boot on GCP, because GCP does not support them. Instead, target VMs boot using a small boot disk, the BDM Boot Disk, which is about ~20 MB and contains the Citrix Provisioning UEFI boot application.

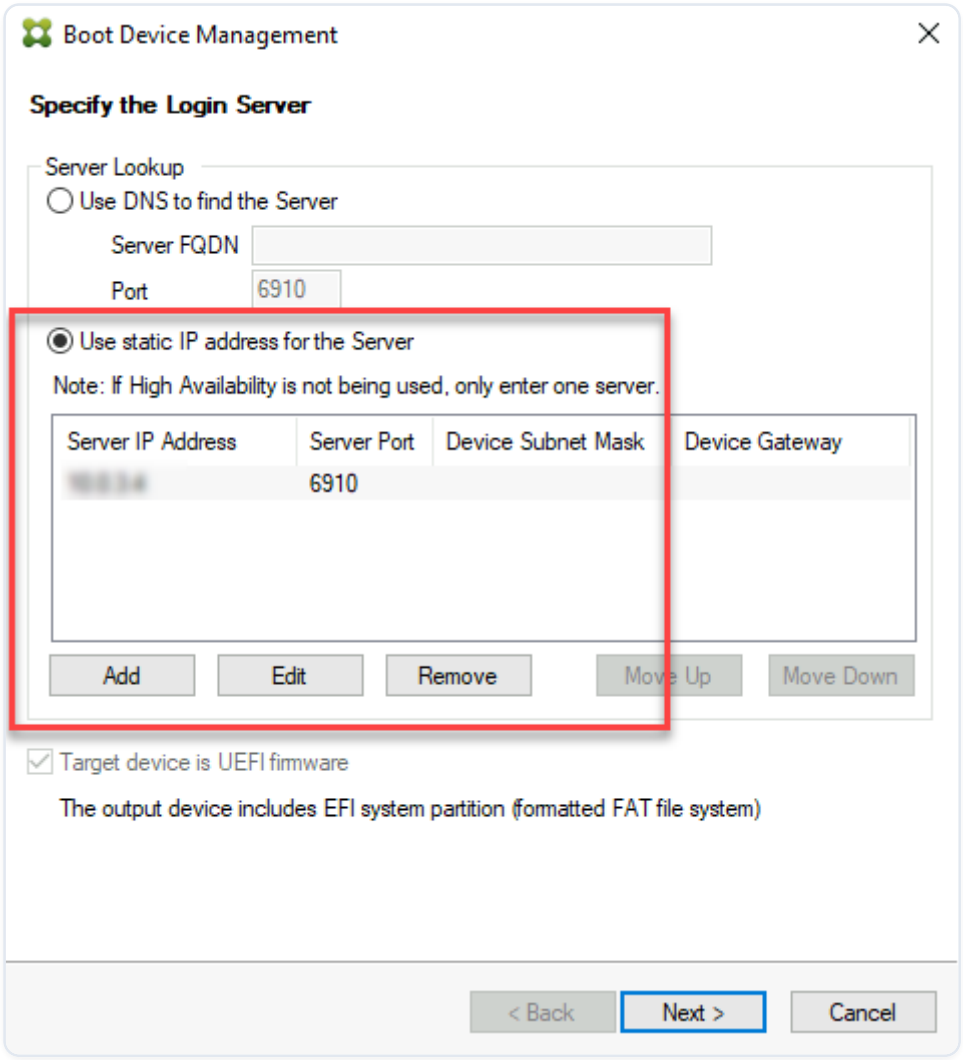
Creating the boot disk

Create the boot disk using the **Boot Device Manager (BDM)** program installed with the server. Run as follows:

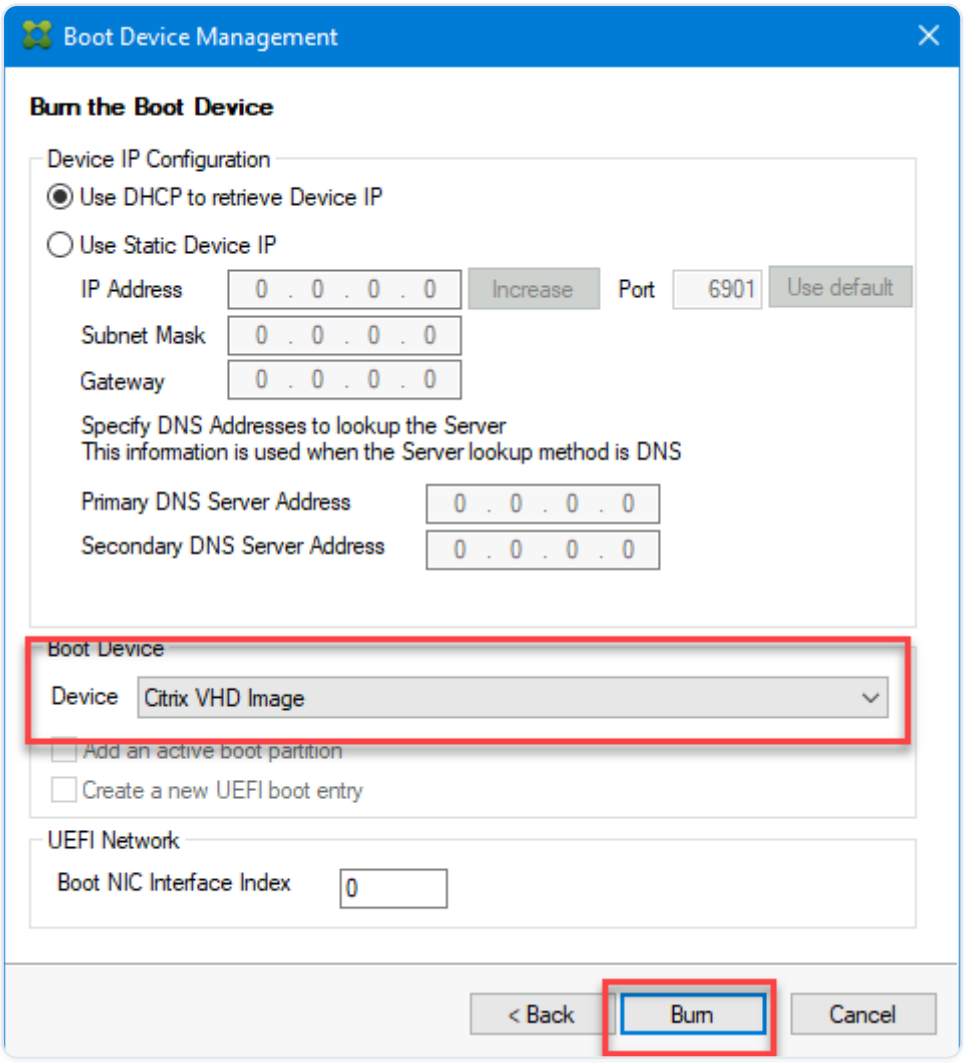
1. Run the **BDM.exe** program.

   ```
   C:\Program Files\Citrix\Provisioning Services\BDM.exe.
   ```

2. Specify the Login server: Enter the Provisioning server information.



3. Create the boot disk VHD file: In the **Device** field, select **Citrix VHD Image**, and click **Burn**.



Target VMs can also use a DNS name to locate the Provisioning server, as opposed to specifying its IP address. To use this feature:

1. Create a DNS entry that maps to the IP addresses used by the Citrix Provisioning servers on the streaming network.
2. Configure the BDM boot disk to contact your Citrix Provisioning servers using this name.

Defining the DNS name to locate the Provisioning server is useful for High Availability (HA), because it allows you to return a list of IP addresses as opposed to configuring all IP addresses in the BDM boot disk. To use this feature:

1. Create a DNS entry that maps to one or more IP addresses used by the provisioning servers on the streaming network.
2. Run the **BDM.exe** program, and specify the DNS host name for the provisioning server DNS on the first page.

Creating the Target VMs

If you want to provision VMs yourself, use the following instructions to create the target VMs:

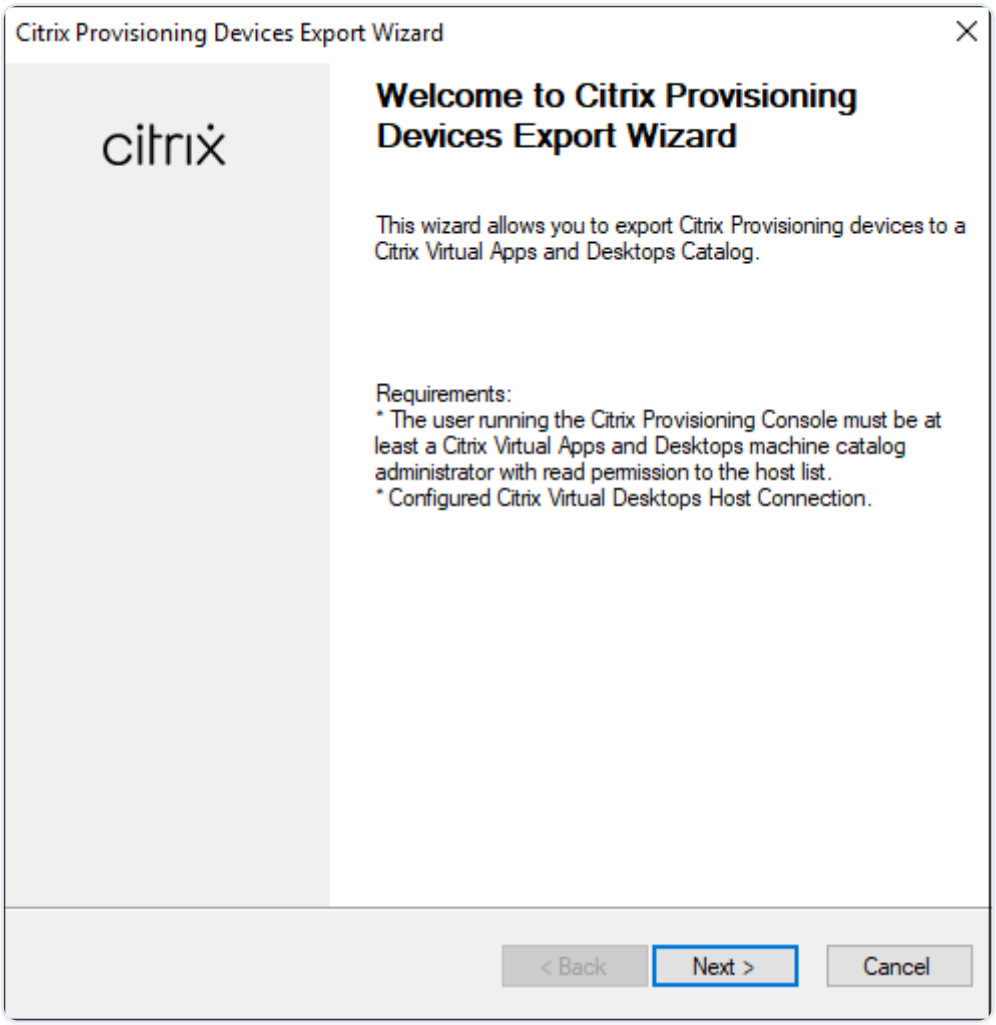
1. Create the BDM boot disk as outlined earlier, and upload the boot disk to a GCP disk. See Import virtual disks for instructions on uploading a VHD to GCP.
2. Create target VMs on GCP using the BDM boot disk that you created, an empty cache disk of the size you need, and connected to a subnet that has access to the provisioning servers.
3. Manage the Target devices in Citrix Provisioning. You can manually add each target VM using the provisioning console or use the Import Wizard to bulk import manually provisioned VMs. Use the GCP console to extract the MAC address assigned to the boot NIC of each manually provisioned target VM. If the IP address assigned to the VM is `n.m.o.p`, then the MAC address is `42:00:nn.mm.oo.pp` (with each component of the IP address in hex).
4. Start each VM once to ensure that the setup is completed. During this boot, Citrix Provisioning formats the cache disk, and then shuts the VM down. Once it is shut down, use the GCP console to deallocate the VM.

Integrate Manually Created Targets with Citrix Virtual Apps and Desktops and Citrix DaaS

Adding a Hosting Connection in Studio connects you to your resource location. The provisioning Export Devices Wizard uses data from this hosting connection to assist it in creating a Broker Catalog.

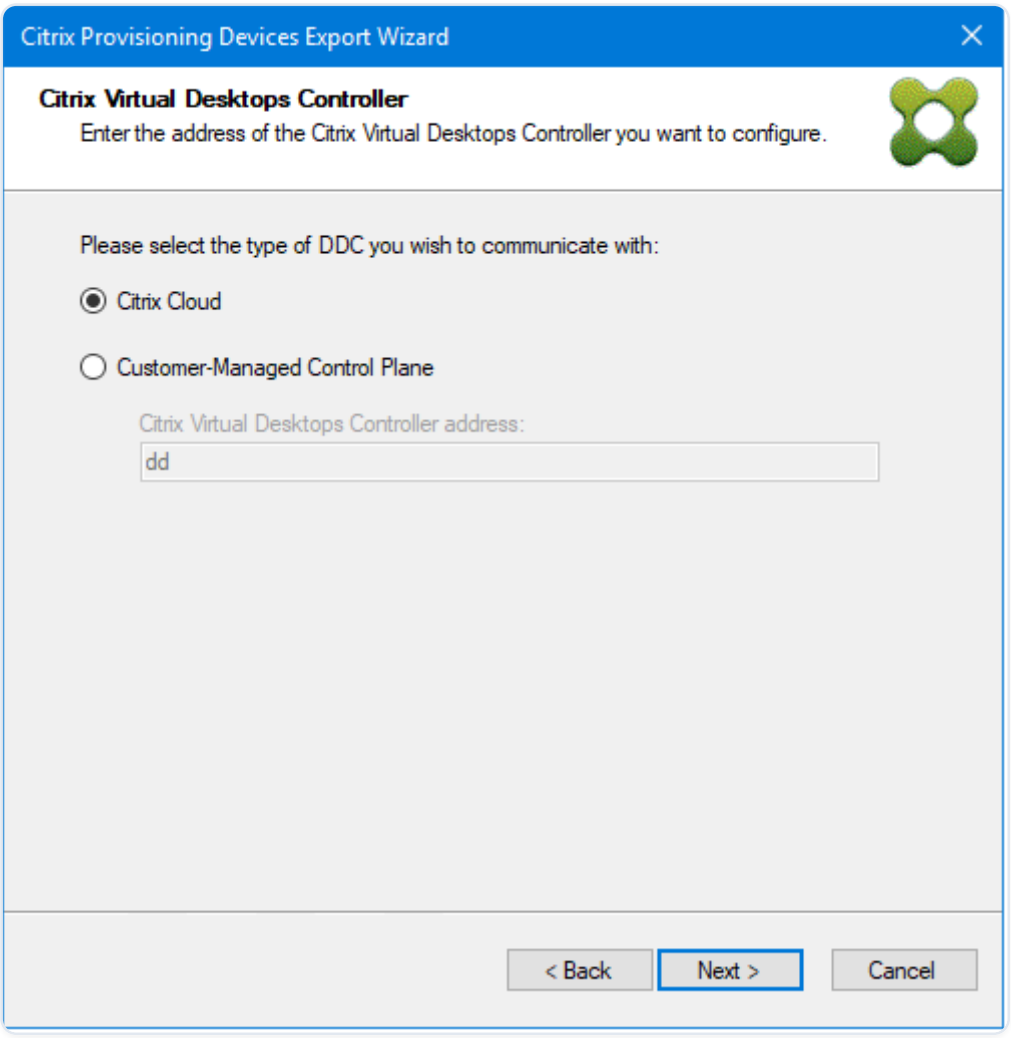
To integrate with Citrix Virtual Apps and Desktops and Citrix DaaS:

1. Launch the **Export Devices** wizard from the Citrix Provisioning console.
2. Click **Next** to start the wizard.

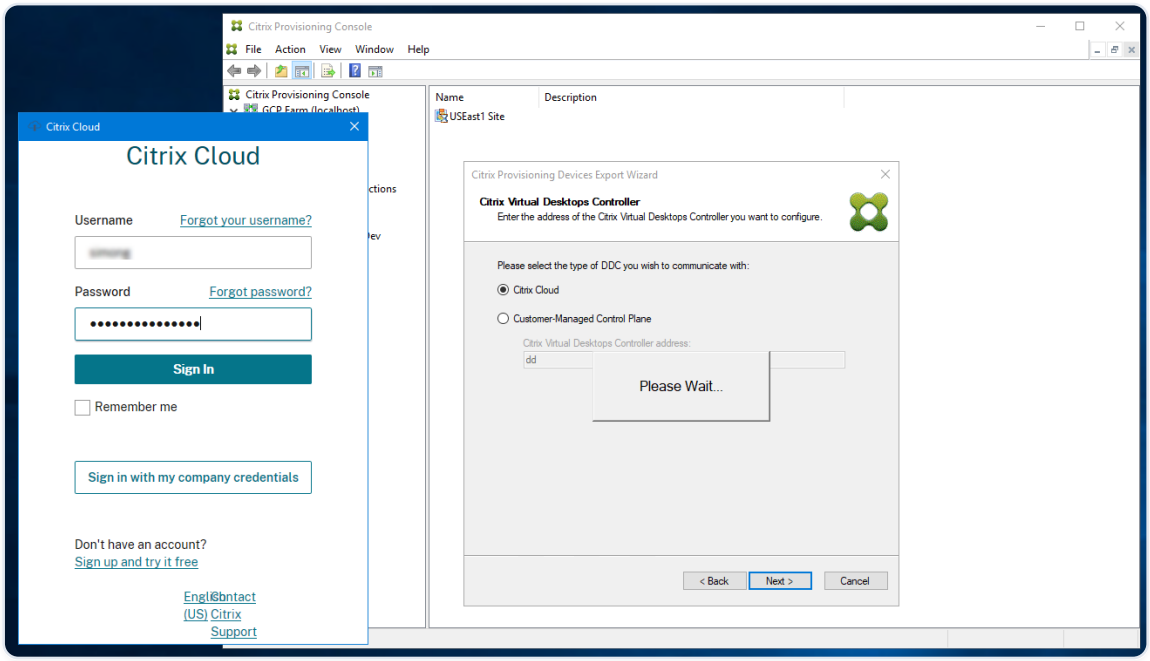


3. Click through the welcome page, select the type of Delivery Controller, and choose **Next**.

    a. If you select **Citrix Cloud**:



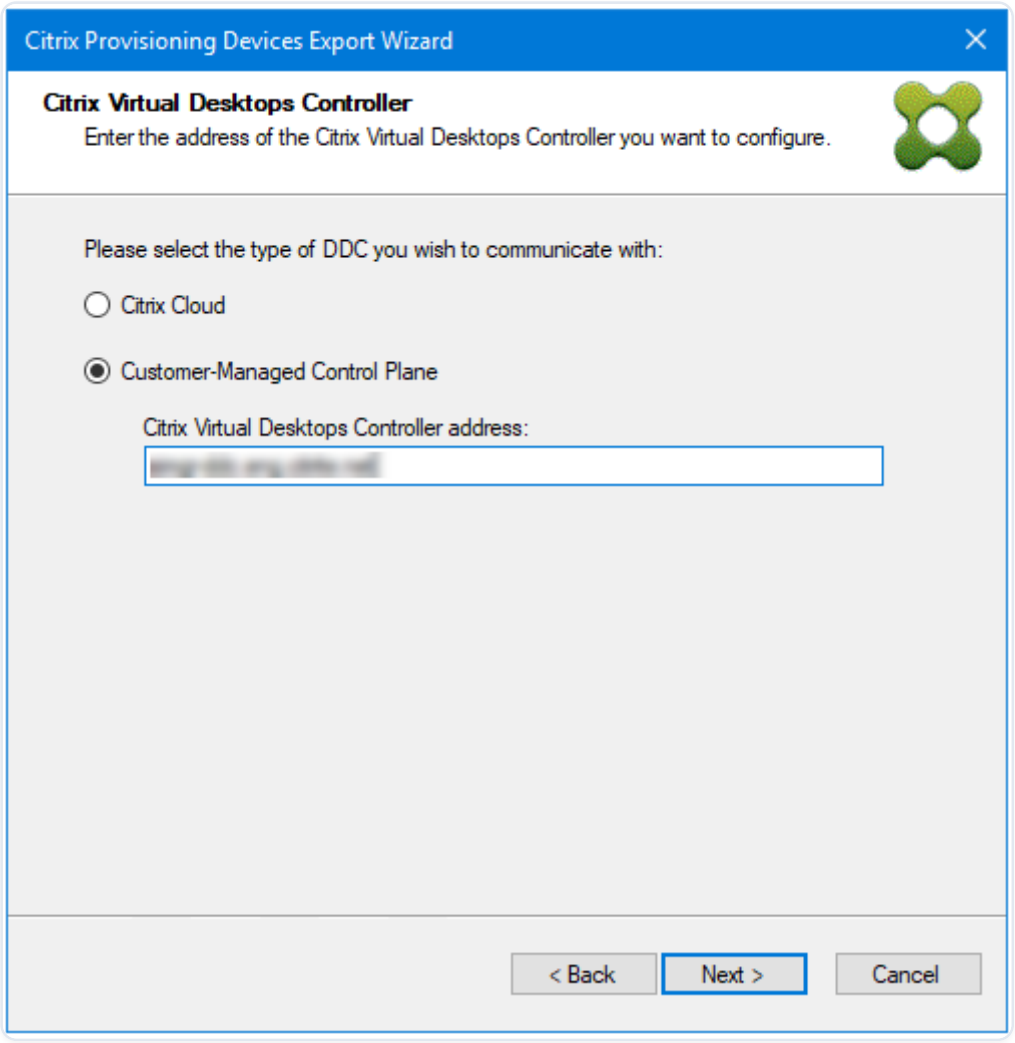
i. Enter Citrix Cloud credentials when prompted



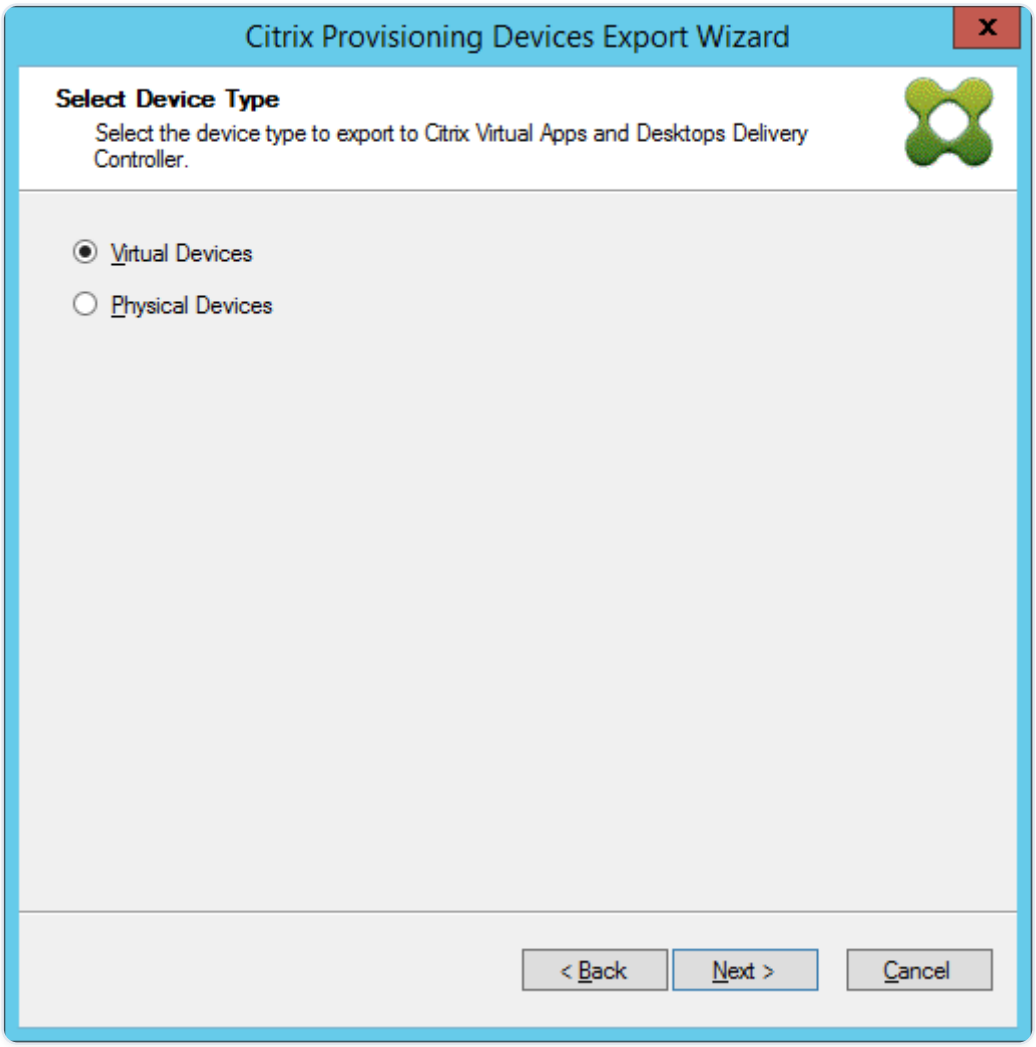
ii. If you have more than one customer, select appropriate cloud customers.

b. If you select **Customer-Managed Control Plane**:

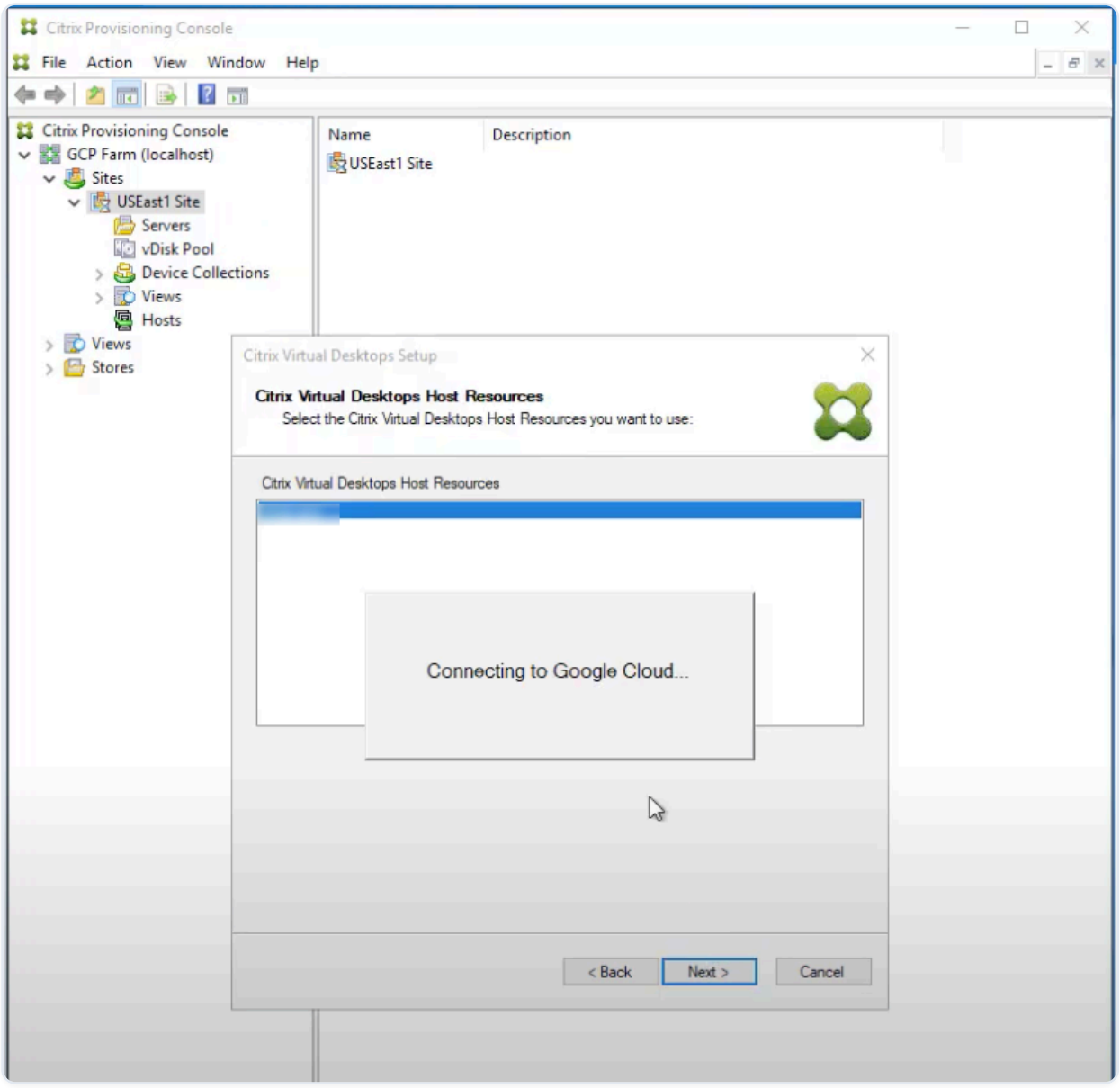
i. Enter the controller hostname or address. The wizard authenticates to the Delivery Controller using the current logged in user.



4. Click the **Device Type** to export. Click **Next**. When selecting **Virtual Devices**, the wizard displays the **Host Resource** screen which allows you to click the host or hypervisor. For physical devices, the wizard skips to the **Active Directory and Collection** selection screen.



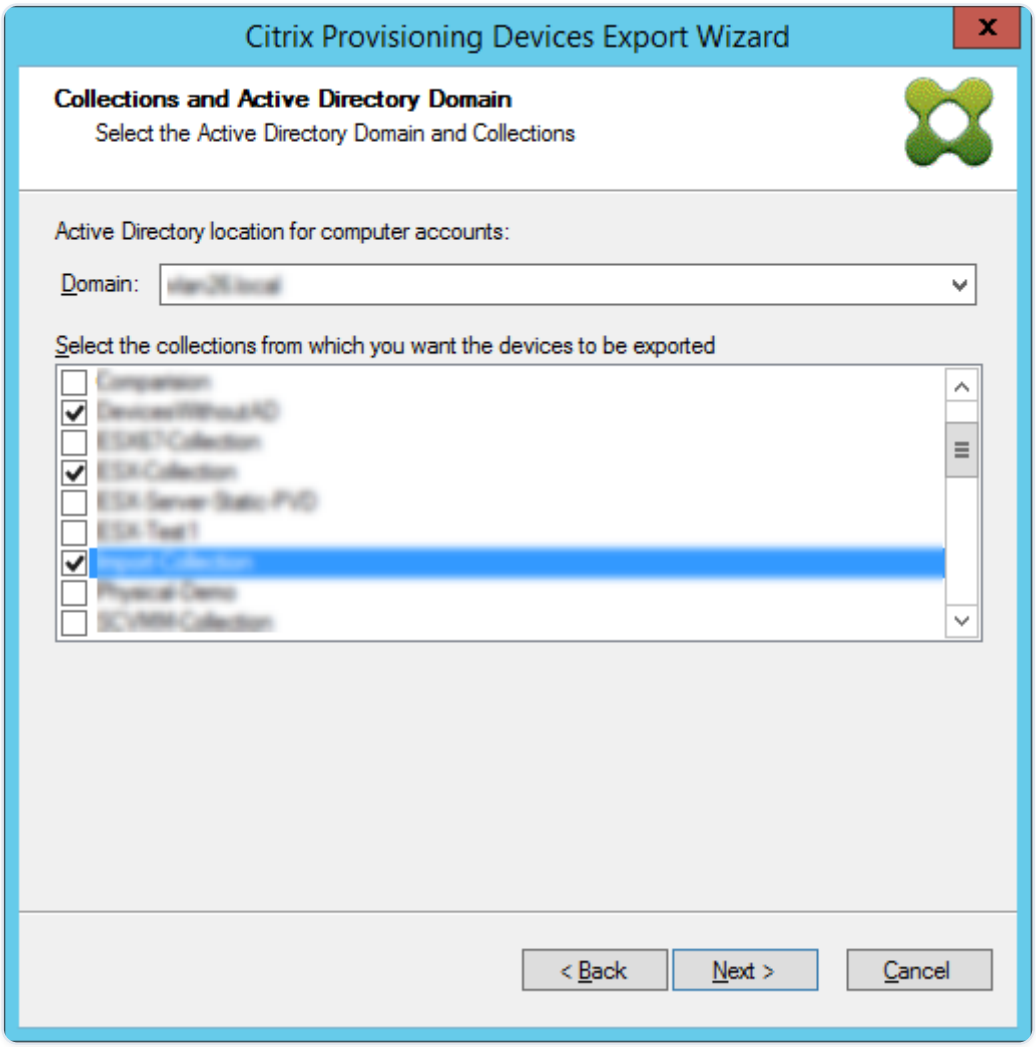
5. On the **Citrix Virtual Desktops Host Resources** screen, select GCP hosting unit. Click **Next**.
6. You receive a message **Connecting to Google Cloud…**. A new web browser opens up. Enter your google credentials to log in to your google cloud.



Note:

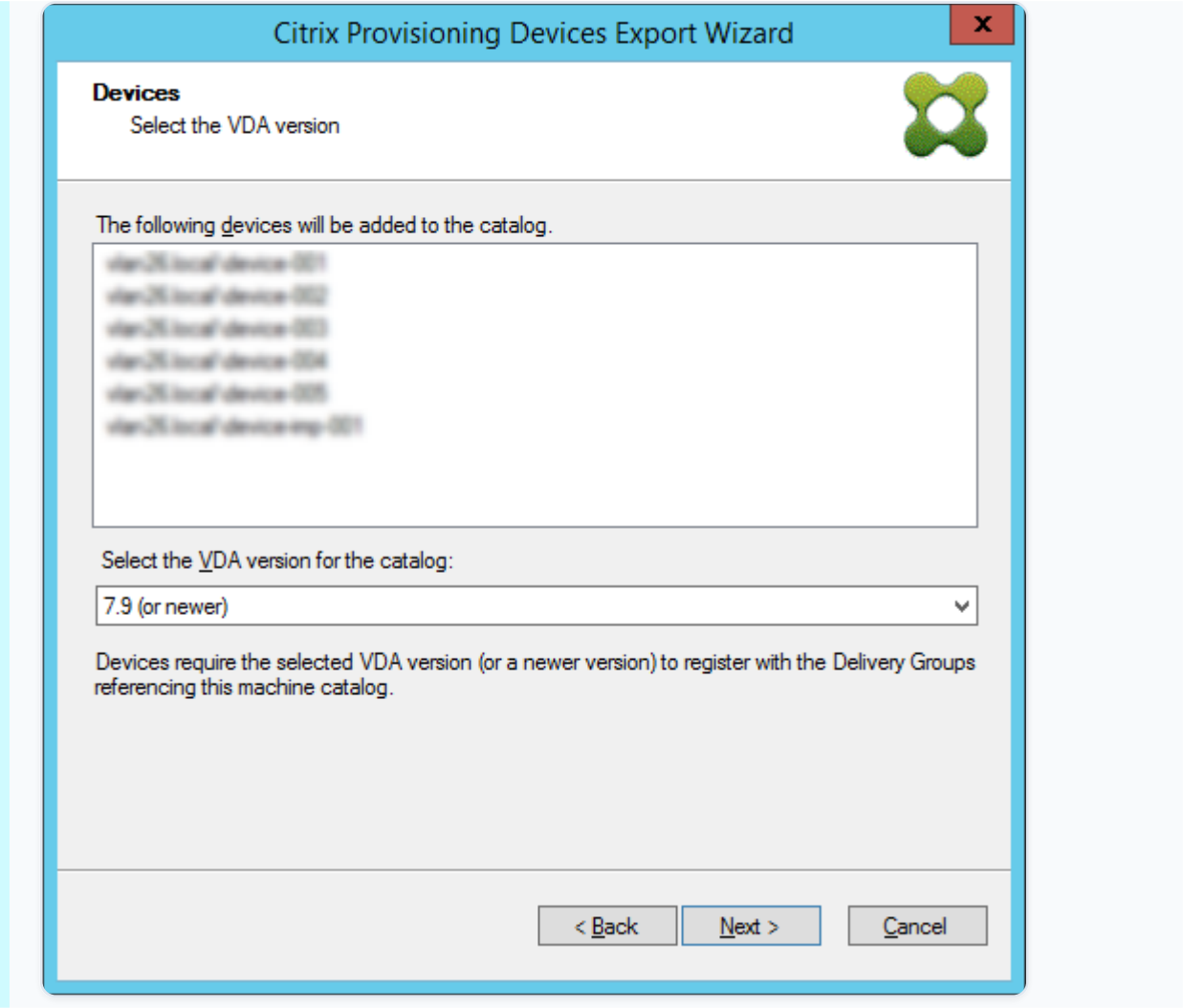
If you previously logged in to the google cloud and approved the permission for the app, the browser to enter your google credentials does not appear.

7. After a successful login, click the Active Directory domain and collections that you want to export. Click **Next**.

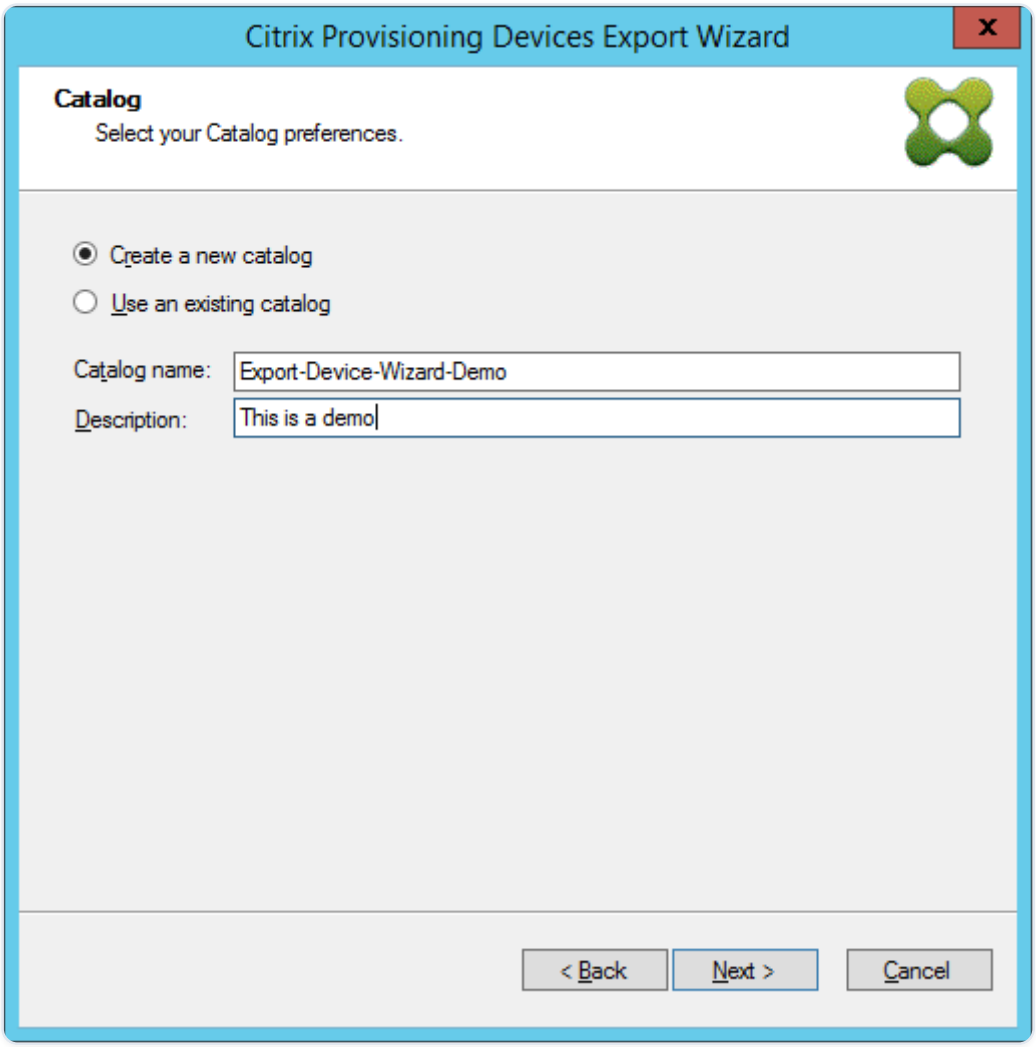


8. Use the list to select the **VDA version**. Devices are required to register with the Delivery Controller referencing the machine catalog. Click **Next**.

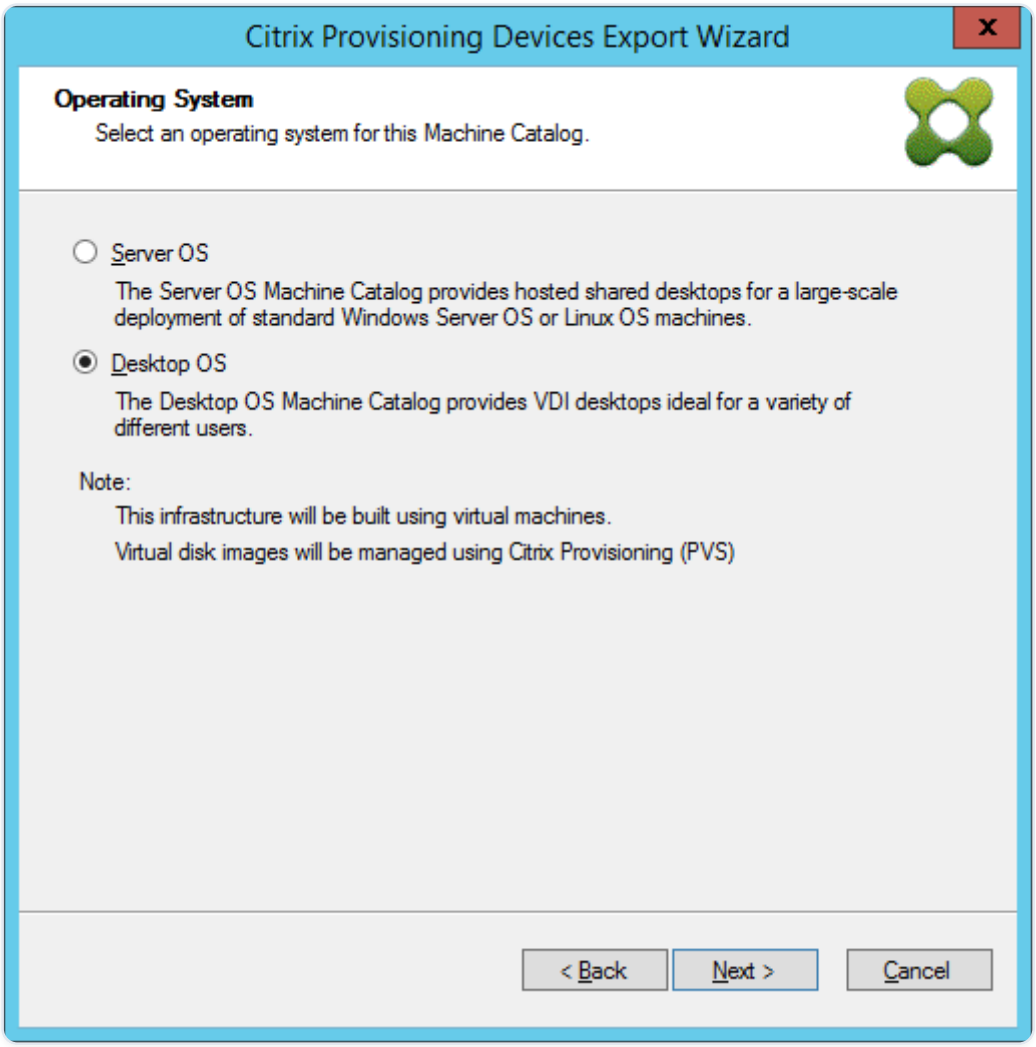
> **Tip:**
>
> All displayed devices are exported to a single Citrix Virtual Apps and Desktops catalog. You cannot select a device in this list.



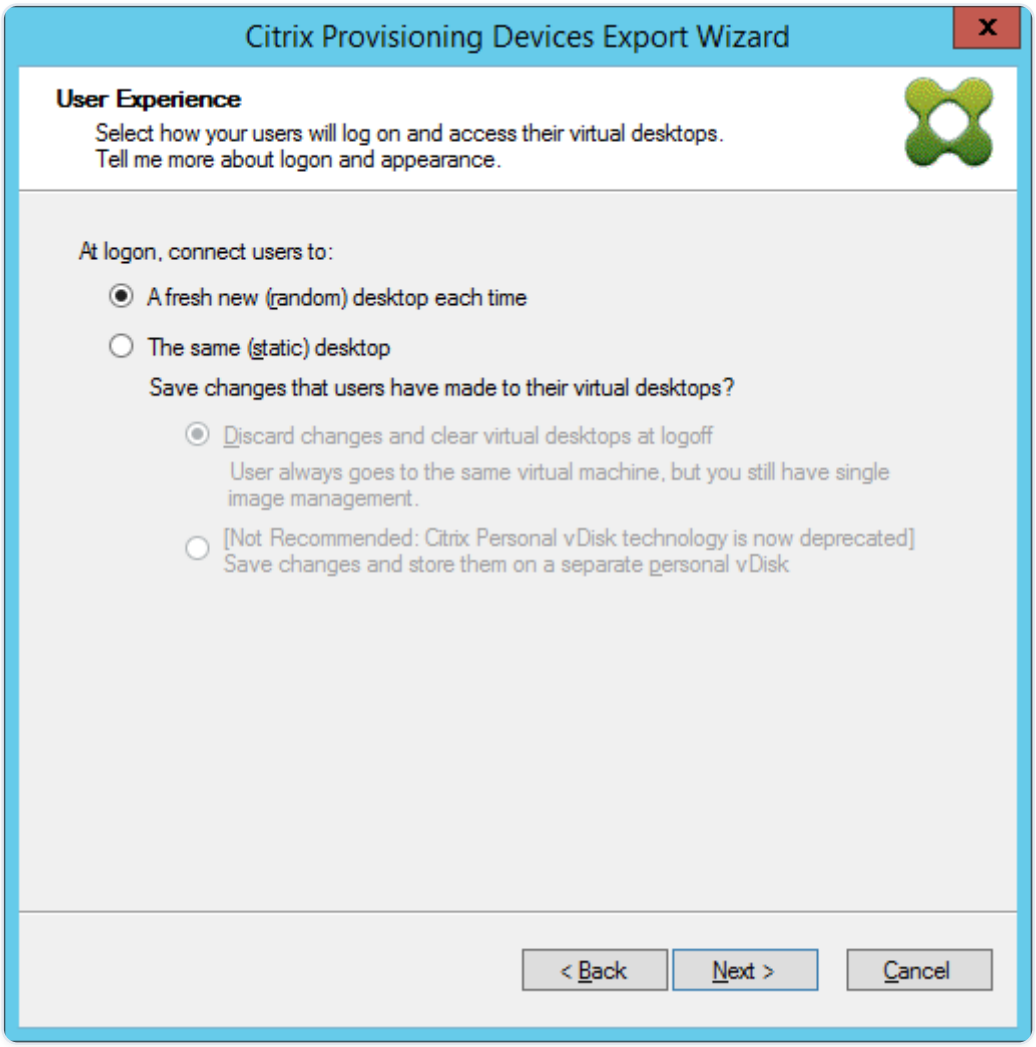
9. Click machine catalog preferences. When creating a catalog, specify the name and optionally include a description. Click **Next**.



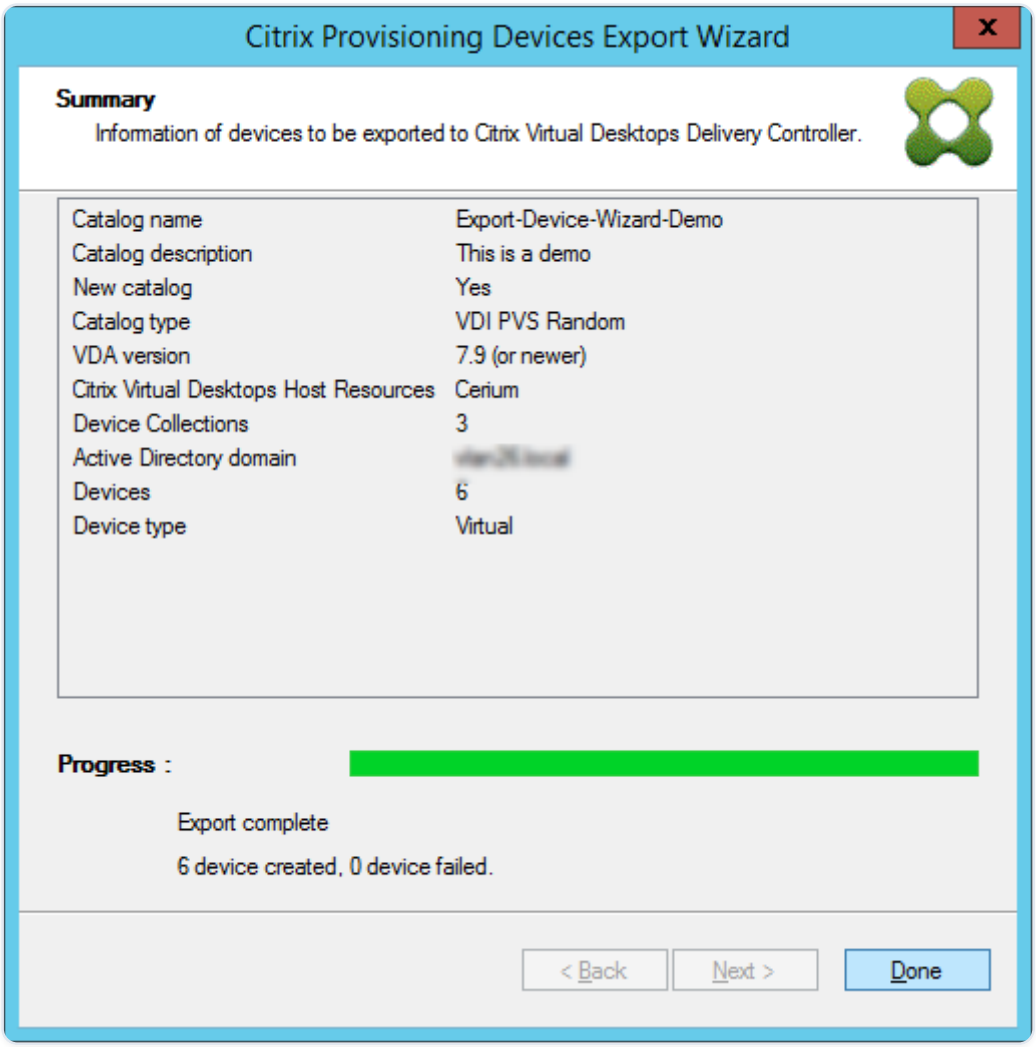
10. Click the operating system. Click **Next**.



11. Set the user experience for the virtual desktop. Click **Next**.



12. Select **Finish** in the **Summary** screen to complete the wizard process.



Note:

The Virtual Hosting Pool data is not added in the Summary screen.

Delete target VMs on GCP

In the Citrix Provisioning console, you can delete target VMs by individually selecting the devices from **Device Collections** or **Views**, or by deleting the entire device collection.

To delete target VMs:

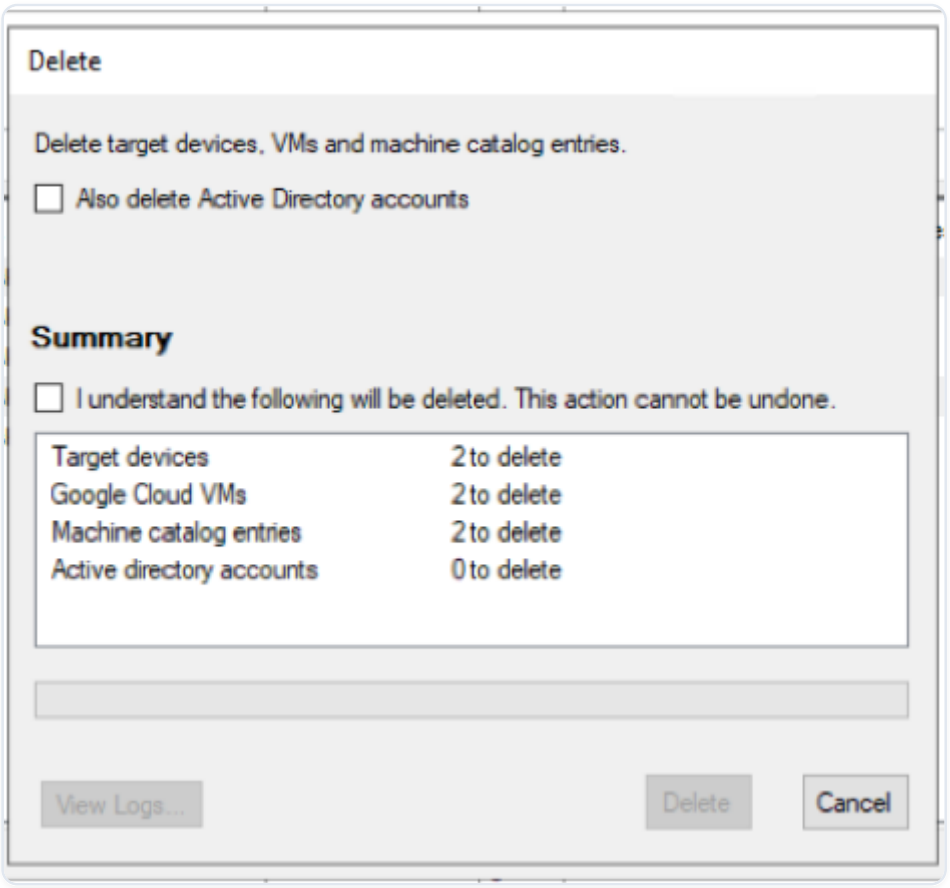
1. Right-click the target VMs from **Device Collections** or **Views** to open a contextual menu.
2. In the contextual menu, click **Delete…**.

Note:

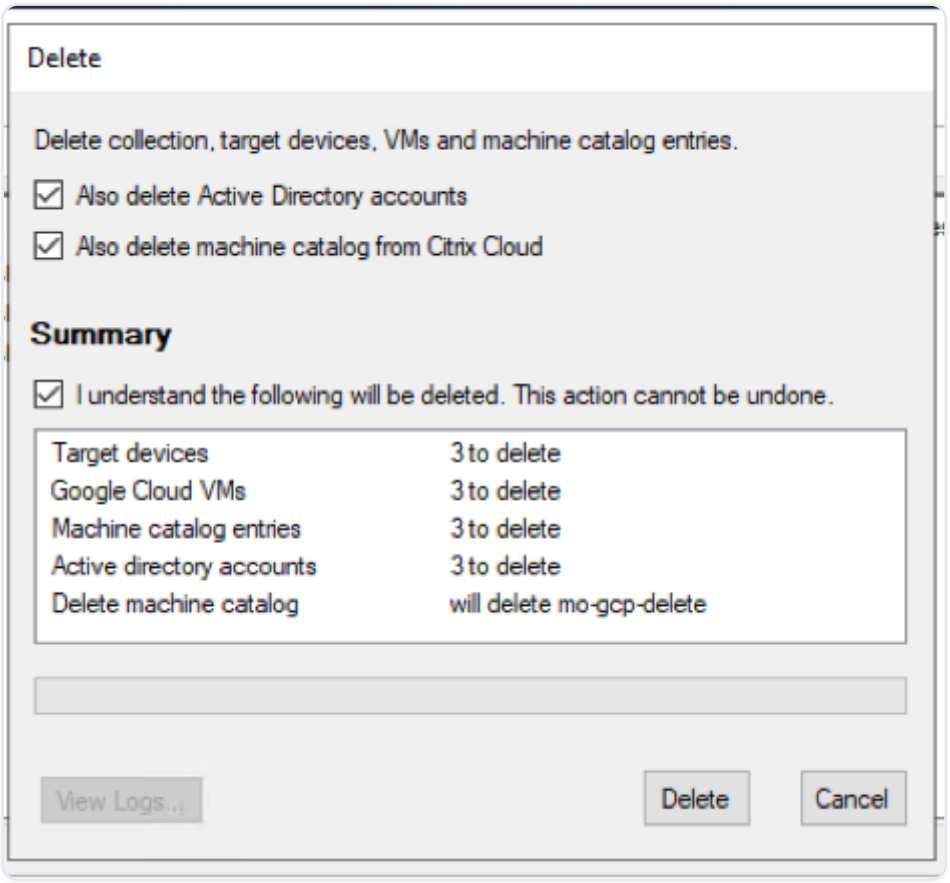
> You cannot delete target VMs that are active. If any of the selected target VMs are active, you do not get **Delete…** option if you select the devices individually. Similarly, if you select the entire device collection and click **Delete..**, you get an error message.

> If any target VM is a GCP VM, the following UI appears:

- If you select VMs individually:



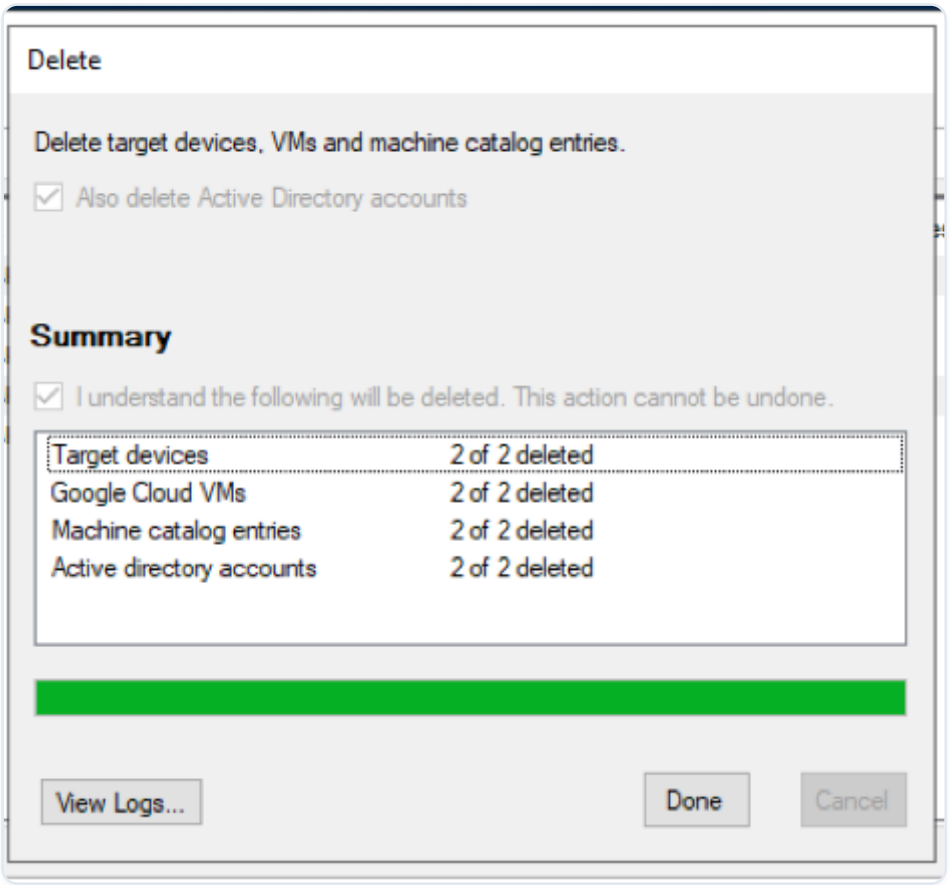
- If you select the entire device collection:

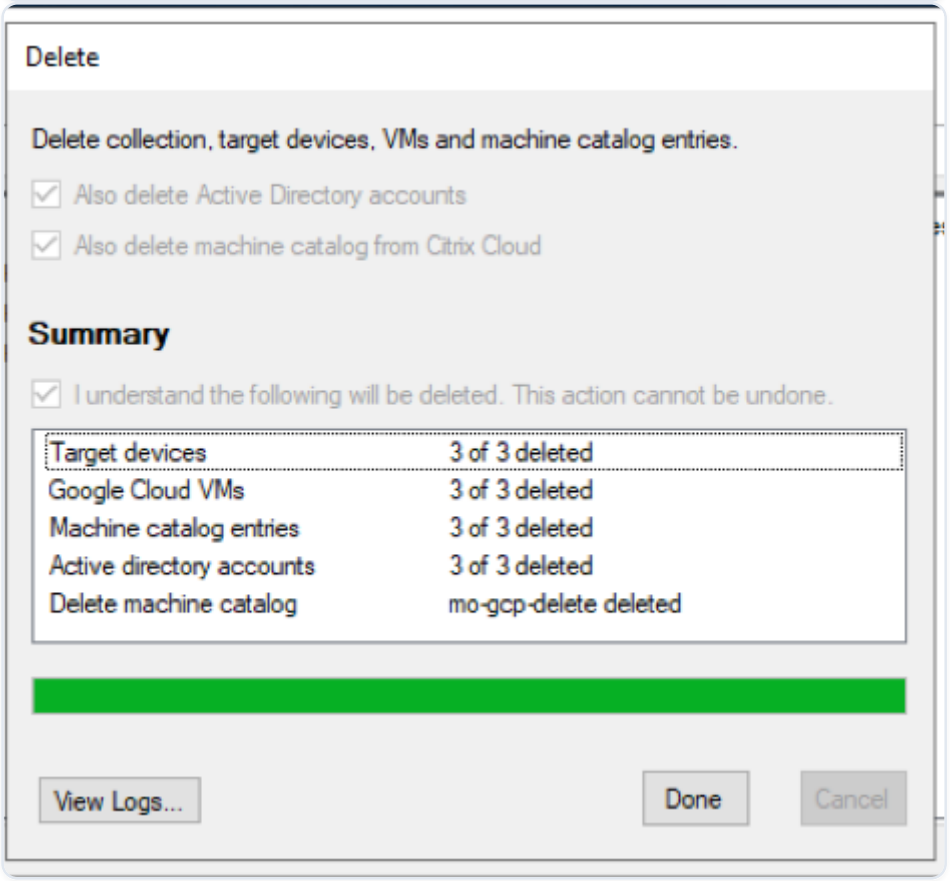


3. By default, target VMs are deleted from the Citrix Provisioning database, GCP, and the Citrix Virtual Apps and Desktops machine catalog. Select the check boxes to delete the target VMs on other associations. The Summary section is updated accordingly.
4. After you click **Delete**, you see a message, **Connecting to Google Cloud…**. A new web browser opens. Enter your Google credentials to log in to your Google Cloud.

> **Note:**
>
> If you have previously logged in to Google cloud and approved the permission for the app, the dialog to enter your Google credentials does not appear.

5. The Summary text area of the **Delete** dialog is updated to reflect the status of the deletion process.





6. When the process completes, click **Done** to close the **Delete** dialog. You can also click **View Logs…** to see the status of the deletion process or save the log file.

Citrix Provisioning™ in Nutanix on AWS

Citrix Provisioning now supports Nutanix clusters on AWS. Nutanix Clusters on AWS offer the same functionality as Nutanix on-premises cluster.

This article describes the procedure for configuring Citrix Provisioning in Nutanix on AWS.

Create Citrix Provisioning environment

To create a Citrix Provisioning environment in Nutanix, create the following VMs, and join them to a domain in the domain controller VM:

1. Domain controller
2. Provisioning server
    a. Install provisioning server, console, Citrix® licensing, and SQL.
    b. Install Nutanix plug-in in the VM. Select Citrix Provisioning.
3. EFI provisioning target device
4. UEFI target device
5. Connector VM
    a. Install Citrix Cloud Connector™
    b. Install Nutanix plug-in. Select Citrix Cloud™ Connector.

Install an Operating System

To install an operating system in a Nutanix VM:

1. Create a VM with two DVD drives and a hard drive.
2. Load the OS in the first DVD drive and Nutanix ISO in the second DVD drive.
3. Once started in Windows ISO, start the Windows installation. At this point, Windows does not detect the Nutanix SCSI drive.
4. Click load driver, browse to the OS, and select `AMDX64` in the Nutanix ISO. Select `vioscsi.inf`. Windows must now detect the SCSI drive.
5. Continue installing the OS.

Install Nutanix drivers

After the OS is installed, go to the Nutanix ISO, and install the Nutanix **VirtIO** to complete installing all Nutanix drivers including the NIC driver.

Set up DHCP service

1. Once the domain is up, note the domain controller IP.
2. Go to the Nutanix Prism and log in.
3. In the Nutanix drop-down menu settings, under Network, select **Network Configuration**.
4. Select the network your VMs are using, and click **Edit**.
5. Under DHCP Settings, enter the IP address of the domain controller VM in the Domain Name Servers, and click **Save**.

Create host connection

The option for Nutanix in Citrix Studio when creating host connection and resources displays when all connector VMs have Nutanix plug-in installed. This is the requirement even if they are not used in the Nutanix zone.

1. Launch the Citrix Studio.
2. Select the hosting node, and click **Add Connection and Resources**.
3. On the Connection screen, select **Create a new Connection**, and enter the connection address in the format address `https://xxx.xxx.xxx.xxx:9440`.
4. Complete the wizard.

VMware cloud and partner solutions

Citrix Provisioning™ supports the following VMware cloud and partner solutions:

- Azure VMware Solution (AVS)
- VMware Cloud on AWS
- Google Cloud Platform VMware Engine

> **Note**:
>
> The VMware cloud and partner solutions are supported from Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) or if you have a Hybrid Rights License.

Azure VMware Solution (AVS) integration

Citrix Provisioning supports AVS. AVS provides cloud infrastructure containing vSphere clusters created by Azure infrastructure. Leverage Citrix Provisioning to use AVS for provisioning your VDA workload in the same way that you would using vSphere in on-premises enviornments.

Setting up the AVS cluster

To enable Citrix Provisioning to use AVS, do the following steps in Azure:

- Request a host quota
- Register the Microsoft.AVS resource provider
- Network Checklist
- Create an Azure VMware Solution private cloud
- Access an Azure VMware Solution private cloud
- Configure networking for your VMware private cloud in Azure
- Configure DHCP for Azure VMware Solution
- Add a network segment in Azure VMware Solution
- Verify Azure VMware Solution environment

Request host quota for Azure Enterprise Agreement customers

In the Azure portal's **Help + Support** page select **New support request**, and include the following information:

- Issue type:Technical
- Subscription:Select your subscription
- Service:All services > Azure VMware Solution
- Resource:General question
- Summary:Need capacity
- Problem type:Capacity Management Issues
- Problem subtype:Customer Request for Additional Host Quota/Capacity

In the **Description** of the support ticket, incldue the following information in the **Details** tab:

- POC or Production
- Region Name

- Number of hosts
- Any other details

> **Note:**
>
> AVS requires a minimum of three hosts, and recommends that you use redundancy of N+1 hosts.

> After specifying details for the support ticket, select **Review + Create** to submit the request to Azure.

Register the Microsoft.AVS resource provider

After requesting the host quota, register the resource provider:

1. Sign in to the Azure portal.
2. On the Azure portal menu, select **All services**.
3. In the **All services** menu, enter the subscription, and select **Subscriptions**.
4. Select the subscription from the subscription list.
5. Select **Resource providers** and enter **Microsoft.AVS** in the search bar.
6. If the resource provider is not registered, select **Register**.

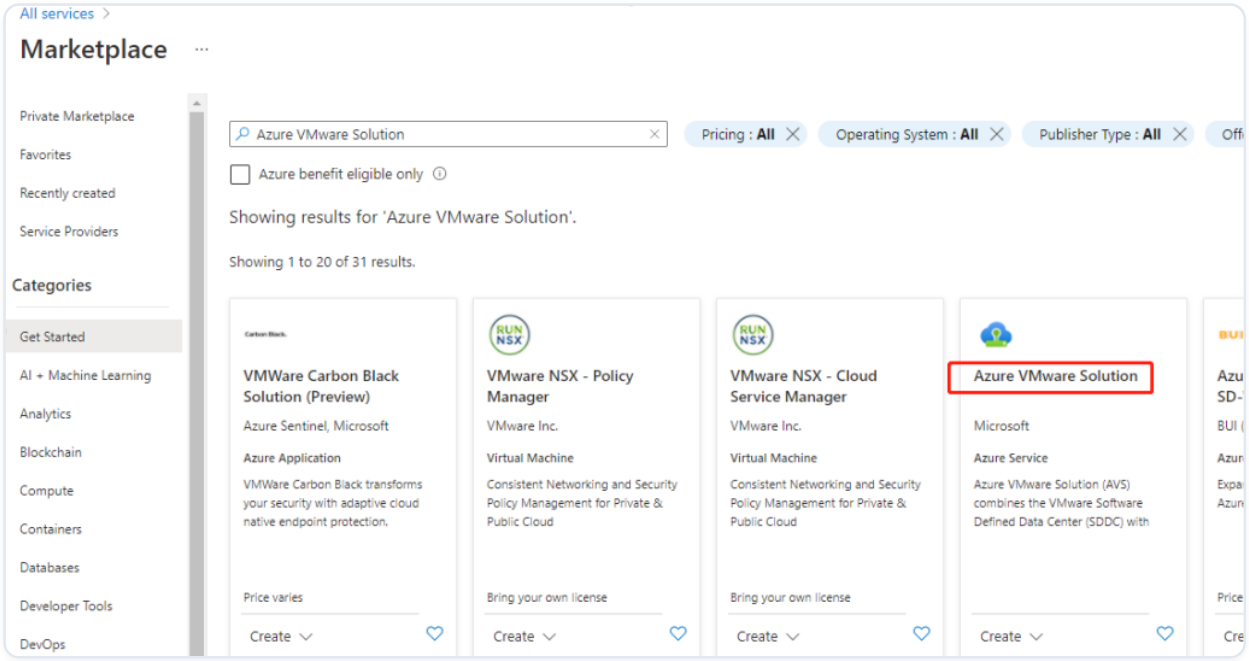
Networking considerations

AVS offers networking services requiring specific network address ranges and firewall ports. See Networking planning checklist for Azure VMware Solution for more information.

Create an Azure VMware Solution private cloud

After conidering network requirements for your environment, create a ASV private cloud:

1. Sign in to the Azure portal.
2. Select **Create a new resource**.
3. In the **Search the Marketplace** text box type, *Azure VMware Solution*, and select **Azure VMware Solution** from the list.



In the **Azure VMware Solution** window:

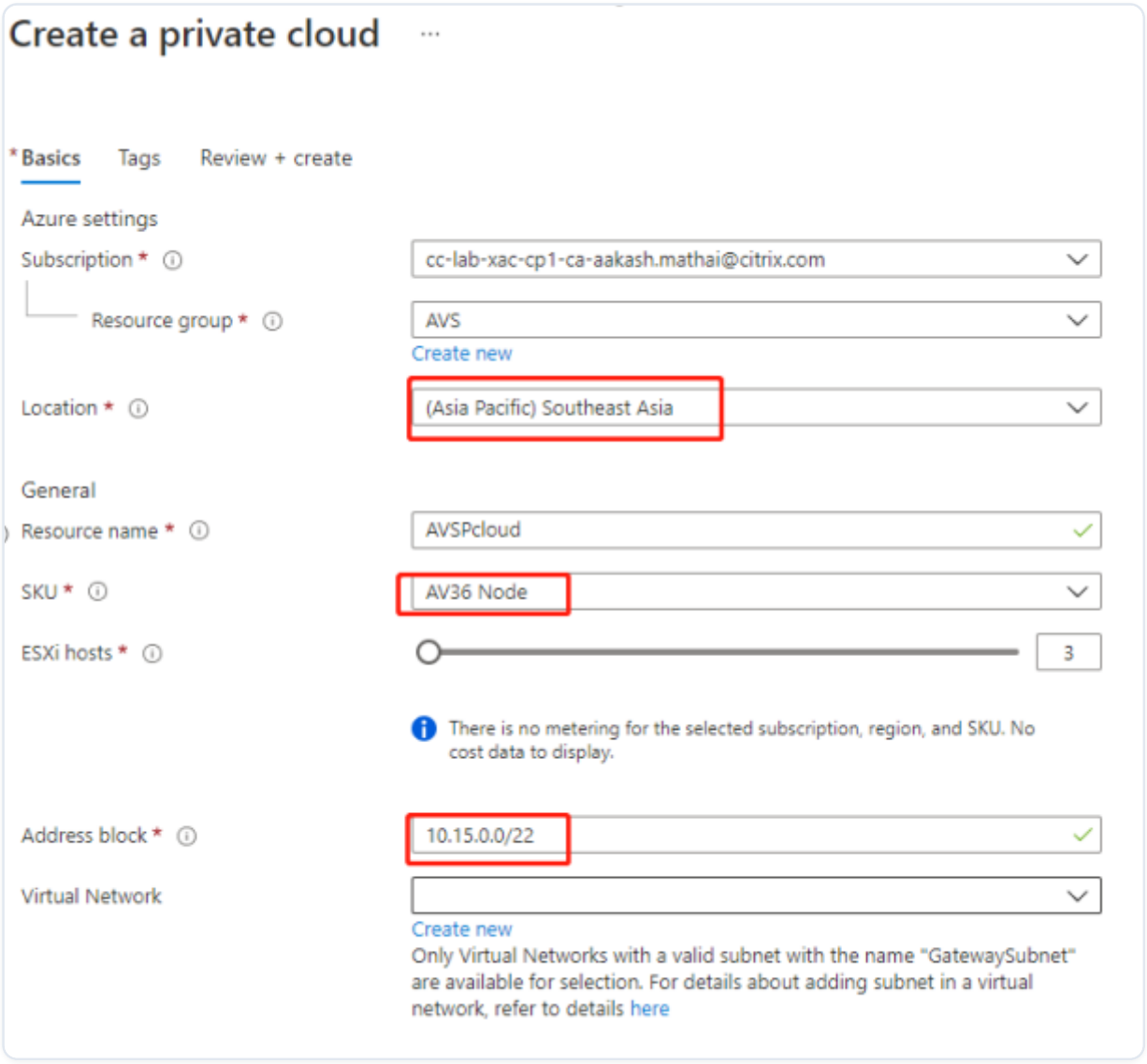
1. Select **Create**.
2. Click the **Basics** tab.
3. Enter values for the fields, using the information in the table below:

FIELD	VALUE
Subscription	Select the subscription you plan to use for the deployment. All resources in an Azure subscription are billed together.
Resource group	Select the resource group for your private cloud. An Azure resource group is a logical container into which Azure resources are deployed and managed. Alternatively, you can create a new resource group for your private cloud.
Location	Select a location, such as east us. This is the region you defined during the planning phase.
Resource name	Provide the name of your Azure VMware Solution private cloud.
SKU	Select AV36.

FIELD	VALUE
Hosts	Shows the number of hosts allocated for the private cloud cluster. The default value is 3, which can be raised or lowered after deployment.
Address block	Provide an IP address block for the private cloud. The CIDR represents the private cloud management network and will be used for the cluster management services, such as vCenter Server and NSX-T Manager. Use /22 address space, for example, 10.175.0.0/22. The address should be unique and not overlap with other Azure Virtual Networks as well as with on-premises networks.
Virtual Network	Leave this blank because the Azure VMware Solution ExpressRoute circuit is established as a post-deployment step.

In the **Create a private cloud** screen:

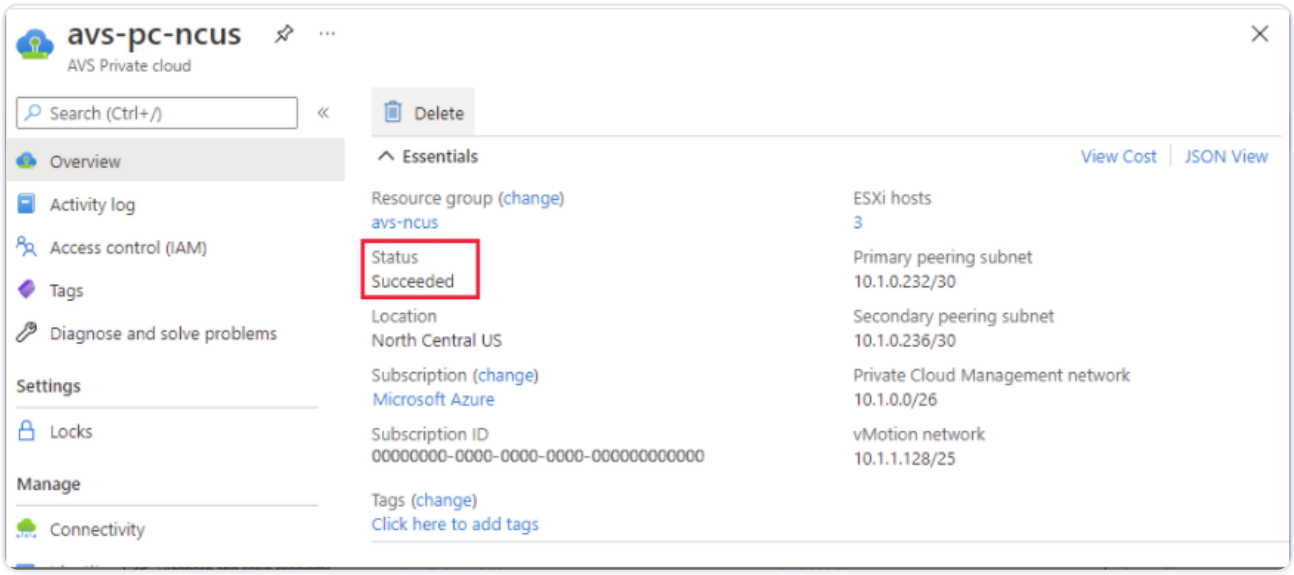
1. In the **Location** field, select the region that has the AVS; the resource group region is the same as the AVS region.
2. In the **SKU** field, select **AV36 Node**.
3. Specify an IP address in the **Address Block** field. For example, 10.15.0.0/22.
4. Select **Review + Create**.
5. After reviewing the information, click **Create**.



Tip:

Creating a private cloud can take 3-4 hours. Adding a single host to cluster can take 30-45 minutes.

Verify that the deployment was successful. Navigate to the resource group you created and select your private cloud. Once the **Status** is **Succeeded** the deployment is complete.



Access an Azure VMware Solution private cloud

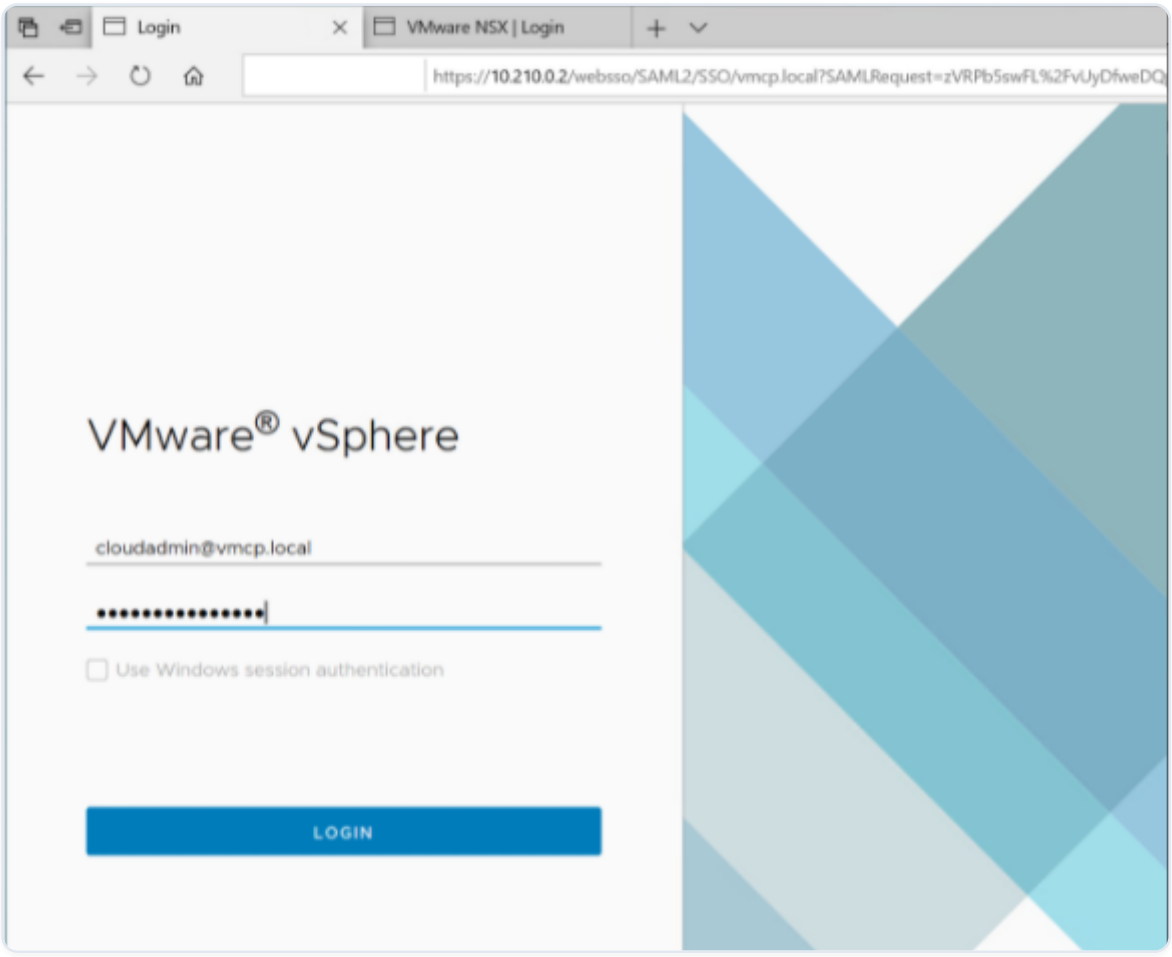
Once you have created a private cloud, create a Windows VM and connect to the local vCenter of your private cloud.

CREATE A NEW WINDOWS VIRTUAL MACHINE

1. In the resource group, select **+ Add** then search and select **Microsoft Windows 10/2016/2019**.
2. Click **Create**.
3. Enter the required information, then select **Review + Create**.
4. Once validation passes, select **Create** to start the virtual machine creation process.

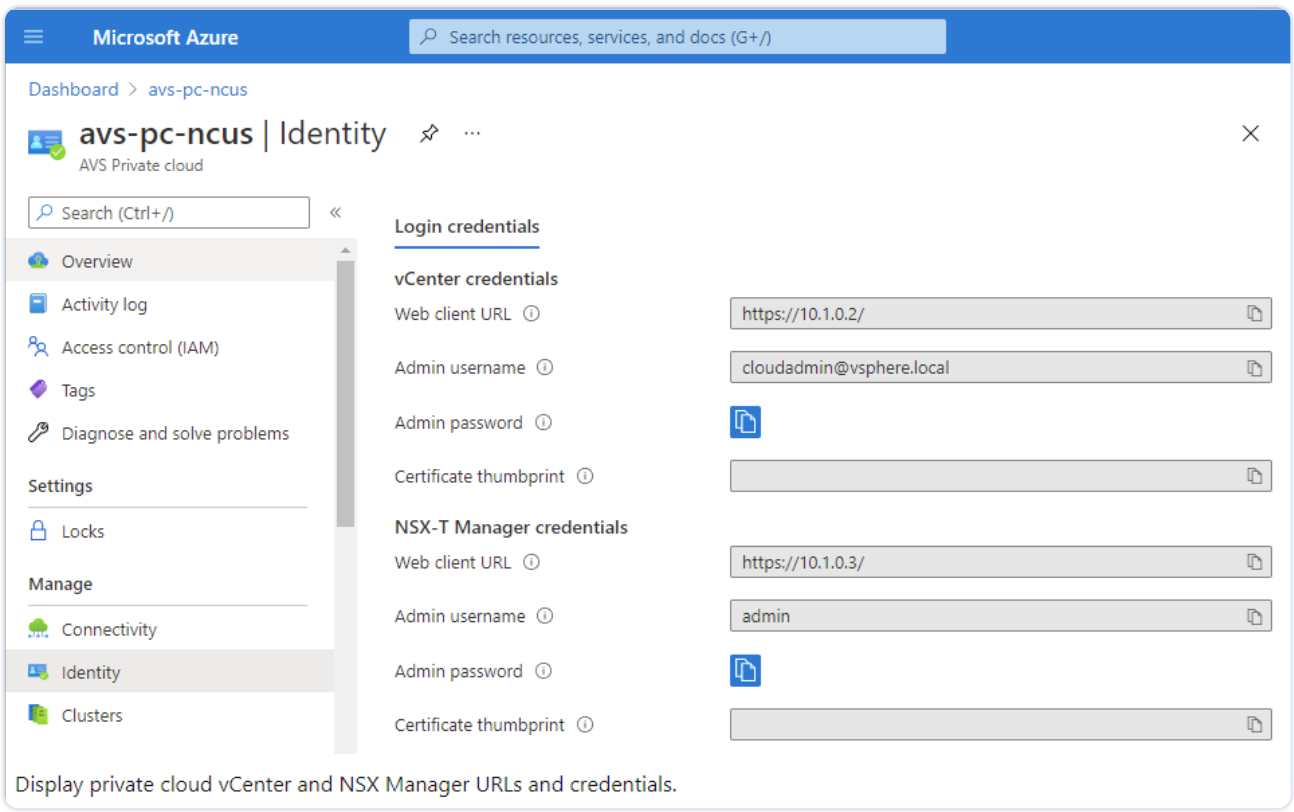
CONNECT TO THE LOCAL VCENTER OF YOUR PRIVATE CLOUD

1. Sign in to **vSphere Client with VMware vCenter SSO** as a cloud administrator.



2. In the Azure portal, select your private cloud, and then **Manage> Identity**.

The URLs and user credentials for private cloud vCenter and NSX-T Manager appear:



Display private cloud vCenter and NSX Manager URLs and credentials.

After confirming URLs and user credentials:

1. Navigate to the VM you created in the preceding step and connect to the virtual machine.
2. In the Windows VM, open a browser and navigate to the vCenter and NSX-T Manger URLs in two browser tabs. In the vCenter tab, enter the mailto:cloudadmin@vmcp.local user credentials from the previous step.

Configure networking for your VMware private cloud in Azure

After accessing an ASV private cloud, configure networking by creating a virtual network and gateway.

CREATE A VIRTUAL NETWORK

1. Sign in to the Azure portal.
2. Navigate to the previously created resource group.
3. Select **+ Add** to define a new resource.
4. In the **Search the Marketplace** text box, type *virtual network*. Find the virtual network resource and select it.
5. On the **Virtual Network** page, select **Create** to set up the virtual network for your private cloud.
6. On the **Create Virtual Network** page, enter the details for your virtual network.
7. On the **Basics** tab, enter a name for the virtual network, select the appropriate region, and click **Next : IP Addresses.**
8. On the **IP Addresses** tab, under IPv4 address space, enter the previously created address.

> **Important:**
>
> Use an address that does not overlap with the address space you used when you created your private cloud.
>
> After entering the address space:

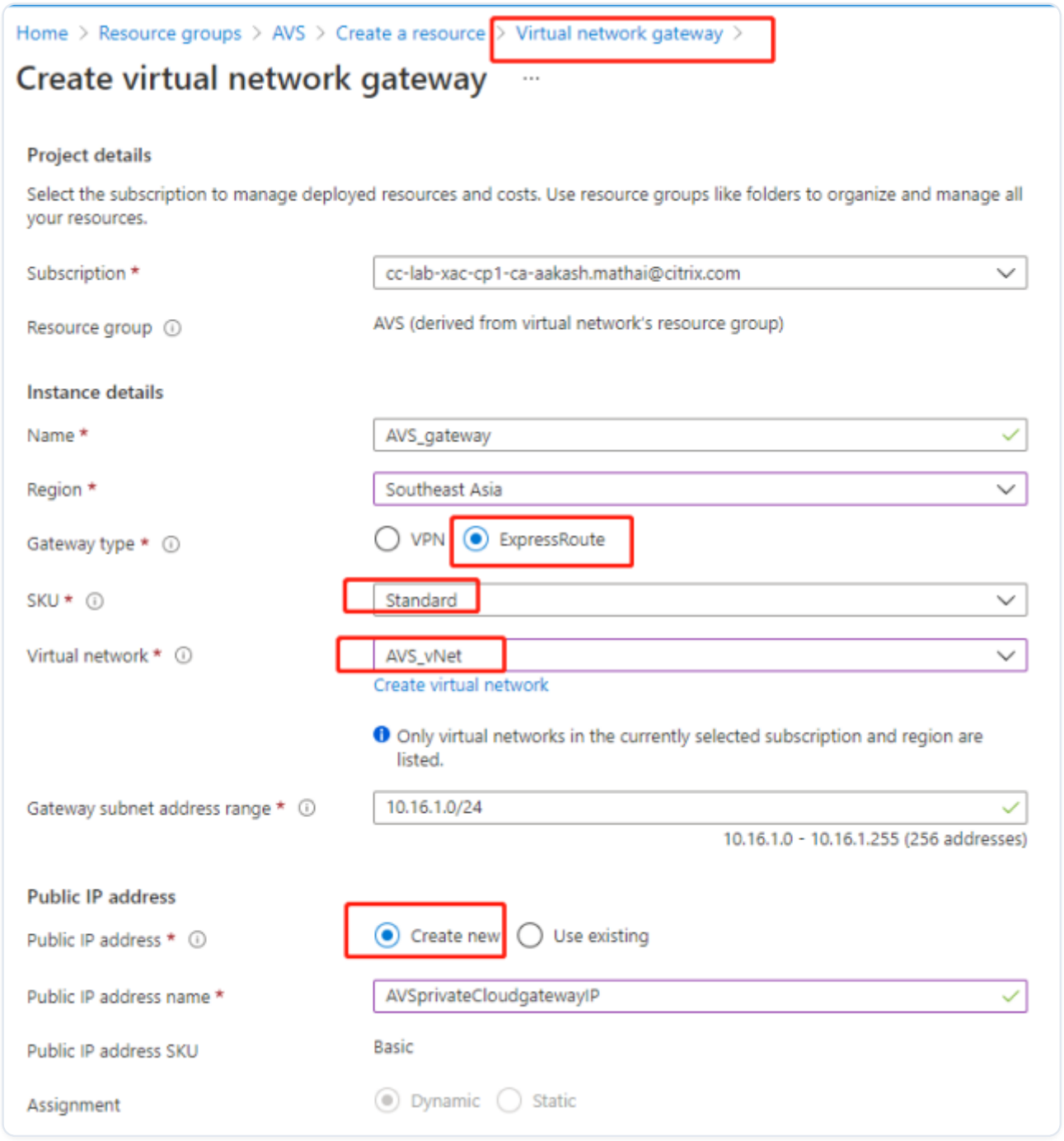
1. Select **+ Add subnet**.
2. On the **Add subnet** page, give the subnet a name and appropriate address range.
3. Click **Add.**
4. Select **Review + create**.

5. Verify the information and click **Create**. Once the deployment is complete, the virtual network appears in the resource group.

CREATE A VIRTUAL NETWORK GATEWAY

After creating a virtual network, create a virtual network gateway.

1. In your resource group, select **+ Add** to add a new resource.
2. In the **Search the Marketplace** text box, type *virtual network gateway*. Find the virtual network resource and select it.
3. On the **Virtual Network gateway** page, click **Create**.
4. On the **Basics** tab in the **Create virtual network gateway** page, provide values for the fields.
5. Click **Review + create**.

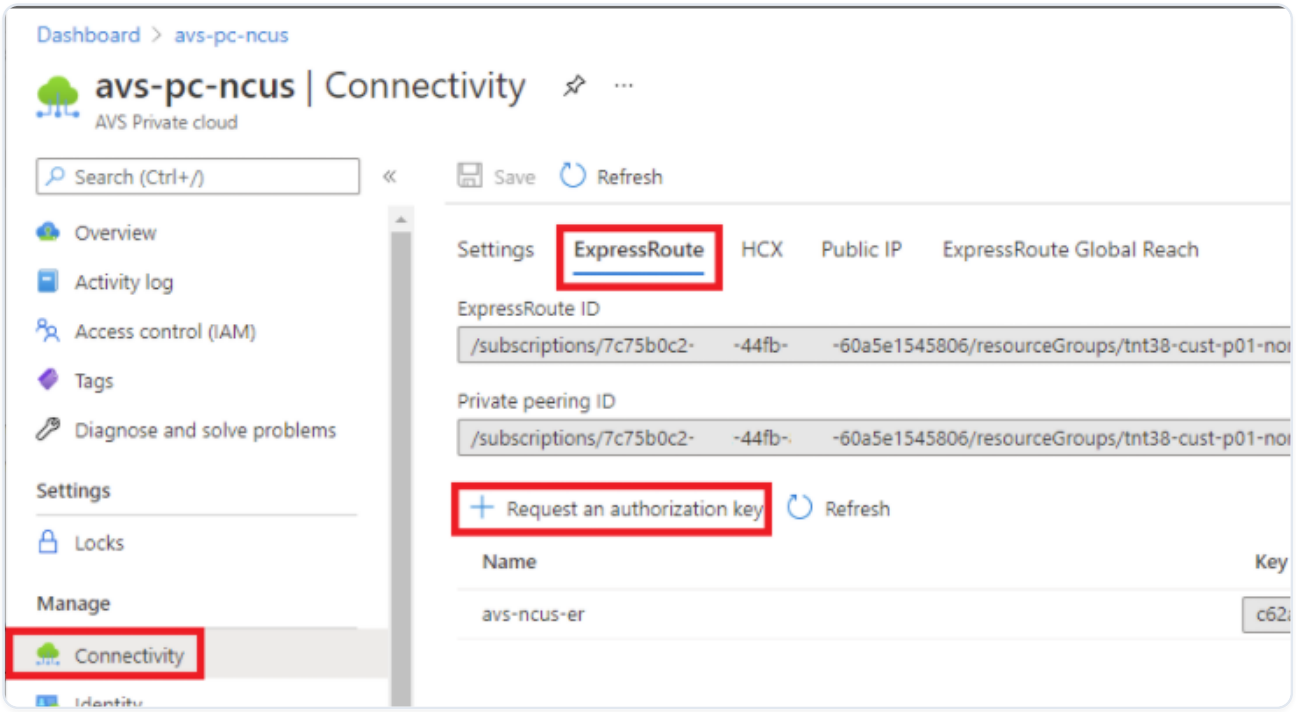


After reviewing the virtual network gateway configuration, click **Create** to deploy your virtual network gateway. Once the deployment completes, connect your **ExpressRoute** connection to the virtual network gateway containing your Azure AVS private cloud.

Connect ExpressRoute to the virtual network gateway

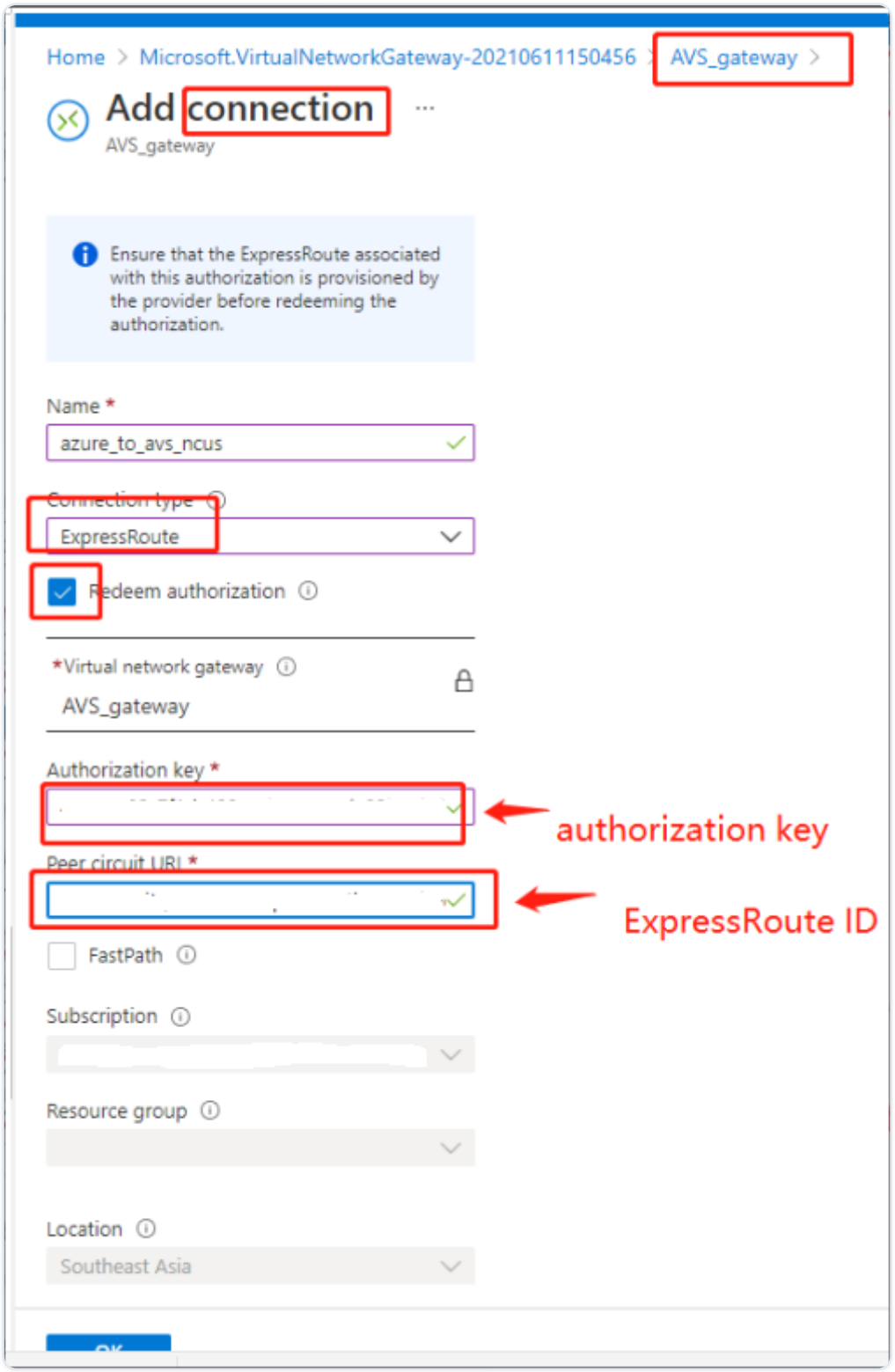
After deploying a virtual network gateway, add a connection between it and your Azure AVS private cloud:

1. Request an ExpressRoute authorization key.
2. In the Azure portal, navigate to the **Azure VMware Solution private cloud**. Select **Manage> Connectivity > ExpressRoute** and then select **+ Request an authorization key.**

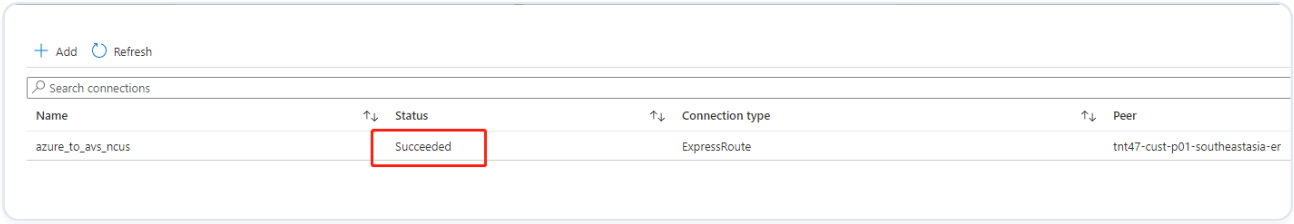


After requesting an authorization key:

1. Enter a name for the key and click **Create**. It may take about 30 seconds to create the key. Once created, the new key appears in the list of authorization keys for the private cloud.
2. Copy the **authorization key** and **ExpressRoute ID**. You'll need them to complete the peering process. The authorization key disappears after some time, so copy it as soon as it appears.
3. Navigate to the **virtual network gateway** you plan to use and select **Connections> + Add**.
4. On the **Add connection** page, provide values for the fields, and select **OK.**



The connection is established between your ExpressRoute circuit and your virtual network:



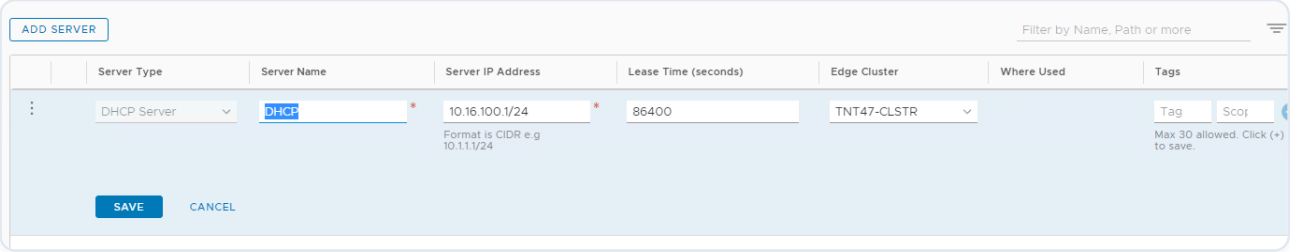
Configure DHCP for Azure VMware Solution

After connecting ExpressRoute to the virutal gateway, configure DHCP.

USE NSX-T TO HOST YOUR DHCP SERVER

In NSX-T Manager:

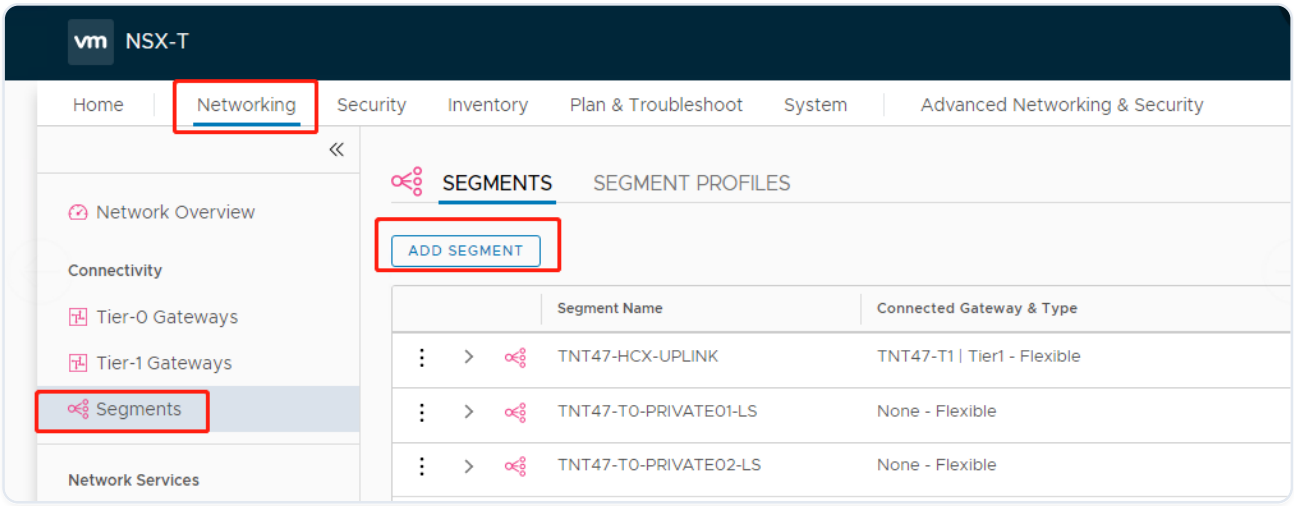
1. Select **Networking> DHCP**, and then select **Add Server**.
2. Select **DHCP** for the **Server Type**, provide the server name and IP address.
3. Click **Save**.
4. Select **Tier 1 Gateways**, select the vertical ellipsis on the Tier-1 gateway, and then select **Edit**.
5. Select **No IP Allocation Set** to add a subnet.
6. Select **DHCP Local Server** for the **Type**.
7. For the **DHCP Server**, select **Default DHCP**, and then click **Save**.
8. Click **Save** again and then select **Close Editing**.



Add a network segment in Azure VMware Solution

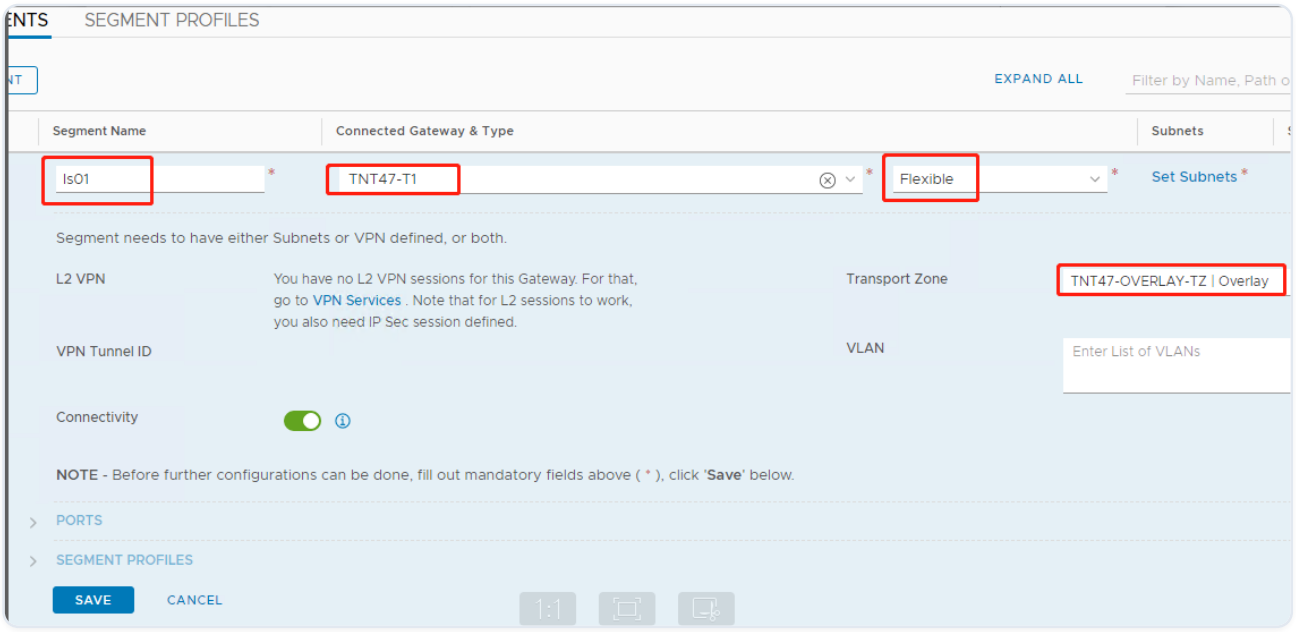
After settnig up DHCP, add a network segment.

To add a network segment, in NSX-T Manager, select **Networking> Segments**, and then click **Add Segment**.



In the **Segments profile** screen:

1. Enter a **name** for the segment.
2. Select the **Tier-1 Gateway (TNTxx-T1)** as the **Connected Gateway** and leave the **Type** as **Flexible**.
3. Select the pre-configured overlay **Transport Zone(TNTxx-OVERLAY-TZ)**.
4. Click **Set Subnets**.



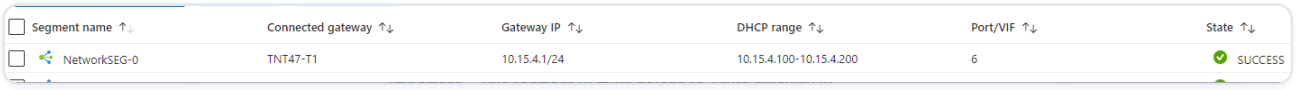
In the **Subnets** section:

1. Enter the gateway IP address.
2. Select **Add**.

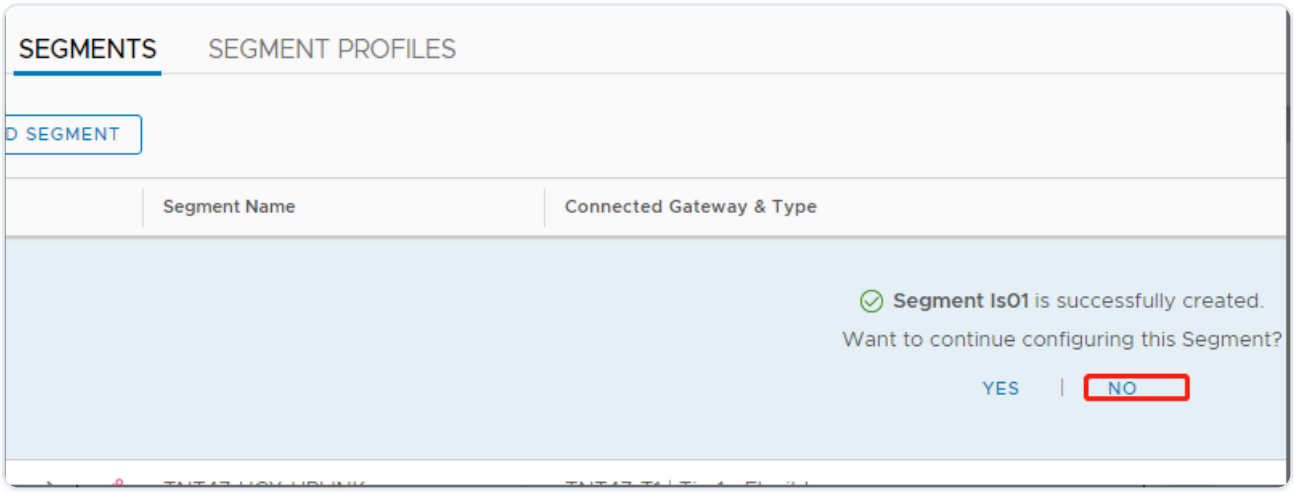
> **Important:**

> This segment IP address must belong to the Azure gateway IP address, 10.15.0.0/22.

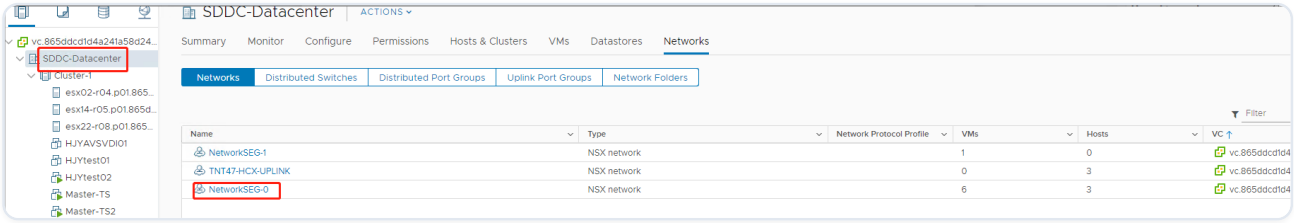
> DHCP range should be belong to segment IP address:



Select **No** to decline the option to continue configuring the segment:

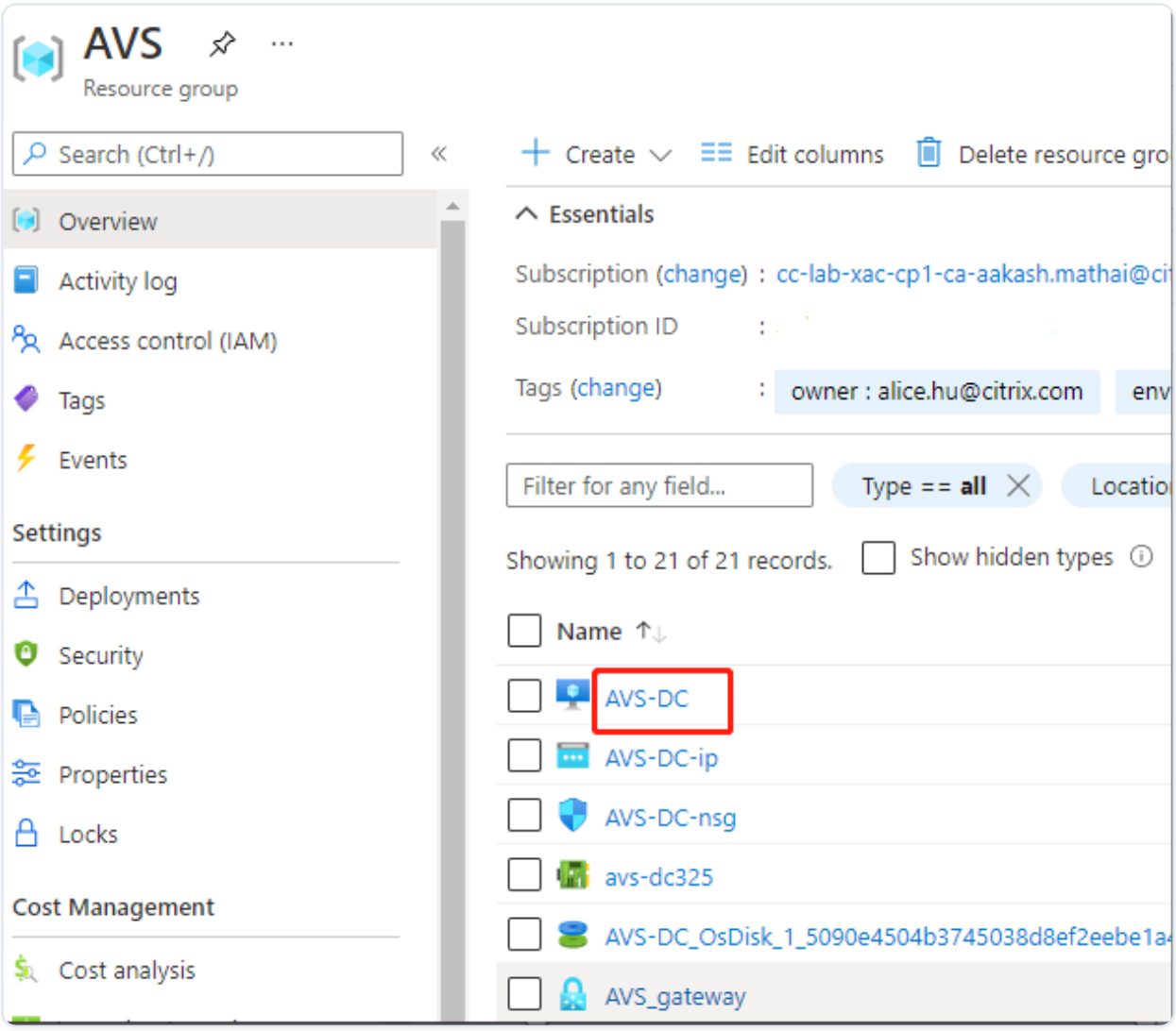


In vCenter, select **Networking > SDDC-Datacenter**:



Verify the Azure AVS environment

1. Setup a direct connection and connector in the Azure resource group:



2. Verify the connection with vCenter credentials.

VMware cloud on AWS

VMware cloud on AWS enables you to migrate VMware based on-premises Citrix workloads to AWS Cloud and your core Citrix Virtual Apps™ and Desktops environment to Citrix DaaS (formerly Citrix Virtual Apps and Desktops service).

Access the VMware cloud environment

1. Log in to VMware cloud services using the URL.
2. Click **VMware Cloud on AWS**. The page **SDDC** appears.
3. Click **OPEN VCENTER**, and then click **SHOW CREDENTIALS**. Note the credentials for later use.
4. Open a Web browser, and enter the URL for the vSphere Web Client.
5. Enter the credentials as noted and click **Login**. The vSphere client webpage is similar to the on-premises environment.

For more and updated information on VMware Cloud on AWS, see VMware Cloud on AWS Documentation.

About VMware cloud environment

There are four views on the vSphere client webpage.

- Host and Cluster view: You cannot create a new Cluster, but the cloud admin can create multiple resource pools.
- VM and Template view: Cloud admin can create many folders.
- Storage View: Select **WorkloadDatastore** storage when you add hosting unit in the Citrix Studio because you have access to only Workload Datastore.
- Network View: The icons are different for VMware cloud networks and opaque networks.

For more and updated information on VMware Cloud on AWS, see VMware Cloud on AWS Documentation.

Set up Citrix Provisioning environment on VMware Cloud on AWS

1. Set up a domain controller or request for credentials for domain vmconaws.local.
2. Use an existing template, or right-click Cluster and select **New Virtual Machine** to create the following three VMs:
    - Citrix Provisioning Server
    - Database Server
    - Cloud Connector for connecting to Citrix DaaS™
3. Create a host connection in Citrix Studio by selecting the **VMware vSphere** option, and select only **WorkloadDatastore** as Storage.

Google Cloud Platform (GCP) VMware Engine

Citrix Provisioning now allows you to migrate VMware based on-premises Citrix workloads to Google Cloud VMware Engine.

This article describes the procedure for configuring the GCP VMware Engine.

Access the VMware Engine portal

1. In the **Google Cloud Console**, click the navigation menu.
2. In the **Compute** section, click **VMware Engine** to open VMware Engine in a new browser tab.

Create first private cloud

Requirements

You must have access to Google Cloud VMware Engine, available VMware Engine node quota, and an appropriate IAM role. Prepare the following requirements before you continue to create your private cloud:

1. Request API access and node quota. For more information, see Requesting API access and quota.
2. Note the address ranges you want to use for VMware management appliances and the HCX deployment network. For more information, see Networking requirements.
3. Get the VMware Engine Service Admin IAM role.

Create your first private cloud

1. Access the VMware Engine portal.
2. On the VMware Engine Home page, click **Create a private cloud**. The hosting location and hardware node types are listed.
3. Select the number of nodes for the private cloud. At least three nodes are required.
4. Enter a Classless Inter-Domain Routing (CIDR) range for the VMware management network.
5. Enter a CIDR range for the HCX deployment network.

> **Important:**
>
> The CIDR range must not overlap with any of your on-premises or cloud subnets. The CIDR range must be /27or higher.

6. Select **Review and create**.
7. Review the settings. To change any settings, click **Back**.
8. Click **Create** to begin creating the private cloud.

As VMware Engine creates your new private cloud, it deploys several VMware components and sets up initial autoscale™ policies for clusters in the private cloud. Private cloud creation can take 30 minutes to 2 hours. After the provisioning is complete, you receive an email.

Setup Google Cloud VMware Engine VPN Gateway

To establish an initial connectivity to Google Cloud VMware Engine, you can use a VPN gateway. This is an OpenVPN-based client VPN using which you can connect to your SDDC's vCenter and do any initial configuration required.

Before deploying VPN gateway, configure the **Edge Services** range for the region where your SDDC is deployed. To do this:

1. Log on to the **Google Cloud VMware Engine** portal, and go to **Network > Regional Settings**. Click **Add Region**.
2. Choose the region where your SDDC is deployed and enable **Internet Access** and **Public IP Service**.
3. Supply the Edge Services range noted during planning and click **Submit**. Enabling these services takes 10–15 minutes.

   Once complete, the Edge Services show as **Enabled** on the Regional Settings page. Enabling these settings allow Public IPs to be allocated to your SDDC, which is a requirement for deploying a VPN gateway.

To deploy a VPN gateway:

1. In the **Google Cloud VMware Engine** portal, go to **Network > VPN Gateways**. Click **Create New VPN Gateway**.
2. Supply the name for the VPN gateway and the client subnet reserved during planning. Click **Next**.
3. Select users to grant VPN access. Click **Next**.
4. Specify the networks that must be accessible over VPN. Click **Next**.
5. A summary screen is displayed. Verify the selections, and click **Submit** to create the VPN Gateway. The VPN Gateways page is displayed with the status of the new VPN gateway as **Creating**.
6. After the status changes to **Operational**, click the new VPN gateway.
7. Click **Download my VPN configuration** to download a ZIP file containing pre-configured OpenVPN profiles for the VPN gateway. Profiles for connecting through UDP/1194 and TCP/443 are available. Choose your preference and import it into Open VPN, and then connect.
8. Go to **Resources** and select your SDDC.

Connect the VPN

Connect to VPN through Azure machine:

1. Create an Azure machine in Azure portal.
2. Download and install the installer **OpenVPN**.
3. Open the **OpenVPN**.
4. Upload the VPN file and connect the VPN.

Create first subnet

Access NSX-T Manager from the VMware Engine portal

The process of creating a subnet happens in NSX-T, which you access through VMware Engine. Do the following to access NSX-T Manager.

1. Log on to the **Google Cloud VMware Engine** portal.
2. From the main navigation, go to **Resources**.
3. Click the **Private cloud name** corresponding to the private cloud where you want to create the subnet.
4. On the details page of your private cloud, click the **vSphere Management Network** tab.
5. Click the **FQDN** corresponding to the NSX-T Manager.
6. When prompted, enter your sign-in credentials. If you have set up vIDM and connected it to an identity source, such as Active Directory, use your identity source credentials.

> **Reminder:**
>
> You can retrieve generated credentials from the private cloud details page.

Set up DHCP service for the subnet

Before you can create a subnet, set up a DHCP service:

In NSX-T Manager:

1. Go to **Networking > DHCP**. The networking dashboard shows that the service creates one Tier-0 and one Tier-1 gateway.
2. To begin provisioning a DHCP server, click **Add Server**.
3. Select **DHCP** for the **Server Type**. Provide the server name and IP address.

4. Click **Save** to create the DHCP service.

Do the following to attach this DHCP service to the relevant Tier-1 gateway. A default Tier-1 gateway is already provisioned by the service:

1. Select **Tier 1 Gateways**, select the vertical ellipsis on the Tier-1 gateway, and then select **Edit**.
2. In the **IP Address Management** field, select **No IP Allocation Set**.
3. Select **DHCP Local Server** for the **Type**.
4. Select the DHCP server that you created for the **DHCP Server**.
5. Click **Save**.
6. Click **Close Editing**.

You can now create a network segment in NSX-T. For more information about DHCP in NSX-T, see the VMware documentation for DHCP.

Create a network segment in NSX-T

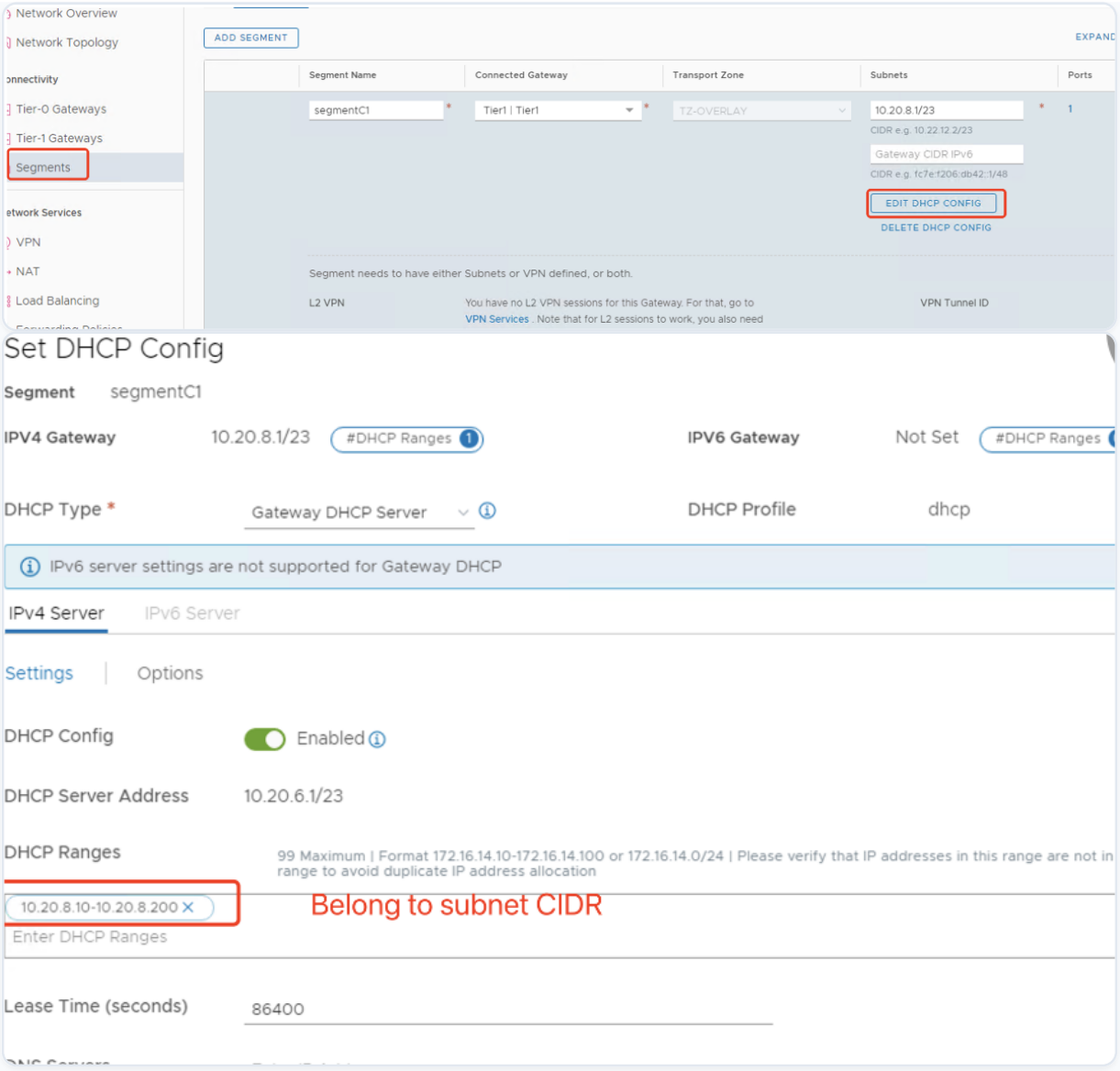
For workload VMs, you create subnets as NSX-T network segments for your private cloud:

1. In NSX-T Manager, go to **Networking > Segments**.
2. Click **Add Segment**.
3. Enter a name for the segment.
4. Select the **Tier-1** as the **Connected Gateway** and leave the Type as **Flexible**.
5. Click **Set Subnets**.
6. Click **Add Subnets**.
7. Enter the subnet range in the **Gateway IP/Prefix Length**. Specify the subnet range with **.1** as the last octet. For example, **10.12.2.1/24**.
8. Specify the DHCP Ranges and click **ADD**.
9. In **Transport Zone**, select **TZ-OVERLAY \| Overlay** from the drop-down list.
10. Click **Save**. You can now select this network segment in vCenter when creating a VM.

In a given region, you can set up at most 100 unique routes from VMware Engine to your VPC network using private services access. This includes, for example, private cloud management IP address ranges, NSX-T workload network segments, and HCX network IP address ranges. This limit includes all private clouds in the region.

> **Note:**

There is a GCP configuration issue because of which you need to configure DHCP range setting several times. Therefore, make sure to configure the DHCP range setting after GCP configuration. Click **EDIT DHCP CONFIG** to configure the DHCP ranges.



Set up Citrix Provisioning environment on Google Cloud VMware Engine

1. Install desktop and server VMs. Run Windows updates for both VMs. Turn them into templates.
2. Create the following VMs:
   - Domain controller with DNS. Be sure to use static DNS pointing to this VM to join the newly created domain.
   - Citrix Provisioning Server
   - SQL Server

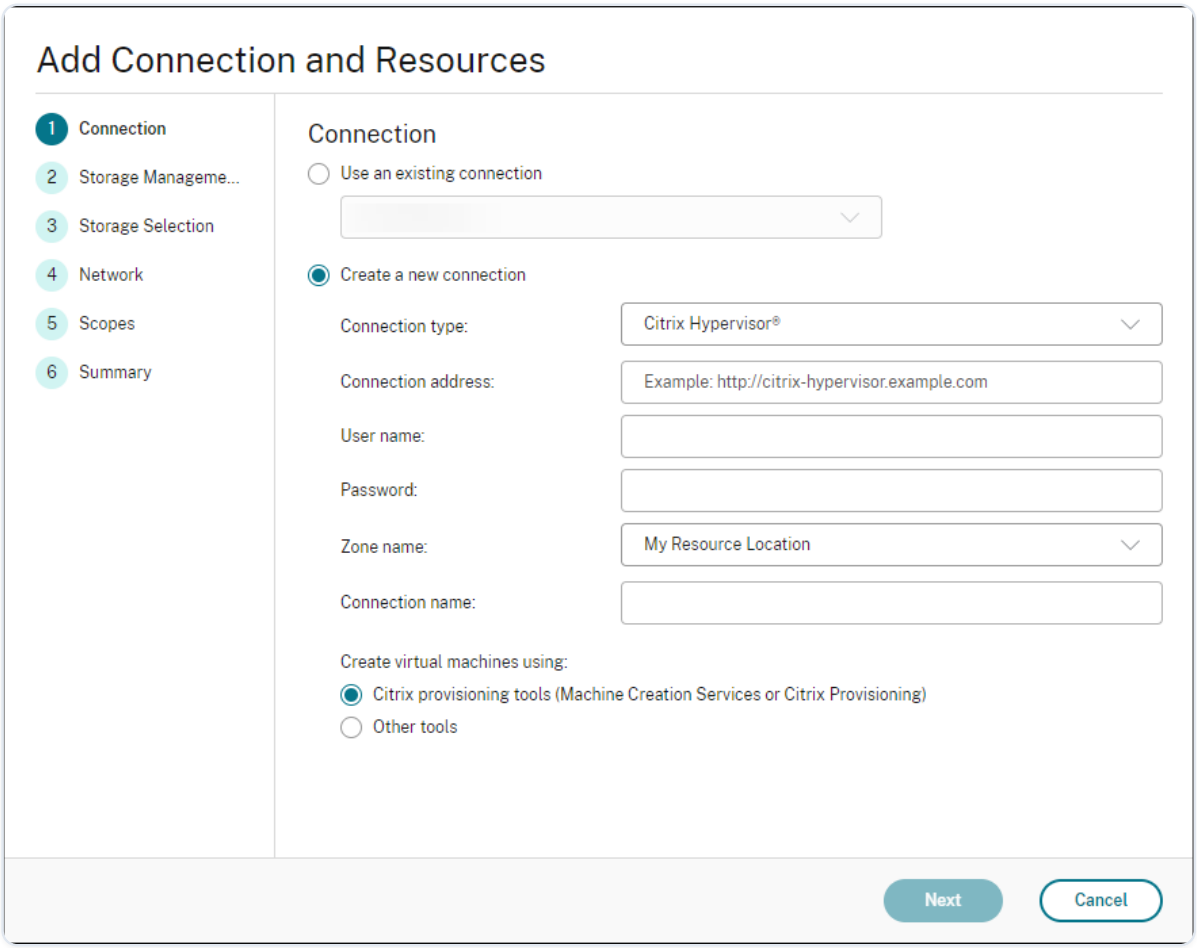
- Connector VM
- UEFI PVS target VM
- EFI PVS target VM

3. Create a host connection in Citrix Studio:

   a. Launch the Citrix Studio.

   b. Select the hosting node, and click **Add Connection and Resources**.

   c. On the **Connection** screen, select **Create a new Connection**, and the following details:



      i. Select **Connection type** as **VMware vSphere**.

      ii. In the **Connection address**, enter the vCenter private IP address.

      iii. Enter the vCenter credentials.

      iv. Enter a connection name.

      v. Choose the tool to create virtual machines.

   d. On the **Network** screen, select the subnet created in NSX-T server.

   e. Click through the screens to complete the wizard.

Export Devices Wizard

This release of Citrix Provisioning includes a new wizard in the provisioning console. The Devices Export Wizard exports existing provisioned devices to the Citrix Virtual Apps and Desktops™ Delivery Controller.

Note:

Instead of importing devices from Citrix Studio, devices are exported to the Delivery Controller using the remote PowerShell SDK. The remote PowerShell SDK can now communicate with both Customer Managed Delivery Controller and Delivery Controller managed by Citrix Cloud. The Devices Export Wizard is the preferred method for adding existing devices in your Citrix Provisioning™ farm to a Citrix Virtual Apps and Desktops Delivery Controller. Ability to import Citrix Provisioning target devices to create catalogs in Citrix Studio is deprecated and removed.

Requirements

The following elements are required for the Export Devices Wizard on Citrix Cloud™ deployments:

- Citrix Virtual Apps™ and Desktops Delivery Controller in Citrix Cloud. The Delivery Controller has its own database where Citrix Provisioning devices are added to the catalog.
- Citrix Cloud Connector™ located on-premises. Used for setting up Citrix Cloud, this connector acts as the relay between Citrix Cloud and the on-premises resource location.
- Citrix Provisioning console. The console uses the Citrix Virtual Apps and Desktops remote PowerShell SDK to add existing Citrix Provisioning devices to the Citrix Virtual Apps and Desktops Delivery Controller.
- Citrix Provisioning server version 1912 or later. This server communicates with the on-premises hypervisors and database and makes SOAP calls to MAPI.

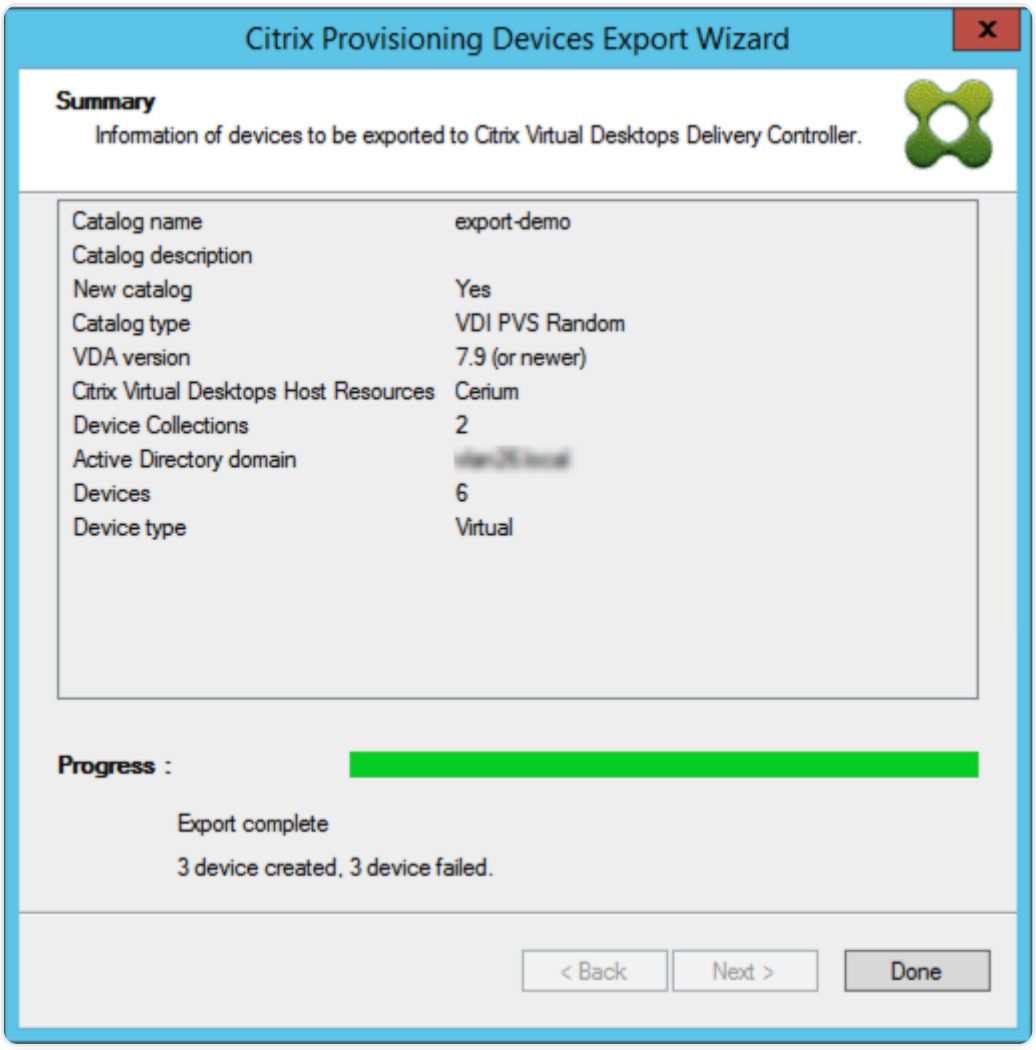
The following elements are required for the Export Devices Wizard on-premises deployments:

- Citrix Provisioning console. The console installer removes any existing installed PowerShell snap-ins and installs the remote PowerShell SDK.
- Citrix Provisioning server version 1912 or later. This server communicates with the on-premises hypervisors and database and makes SOAP calls to MAPI.
- Citrix Virtual Apps and Desktops Delivery Controller for on-premises setup.

Important considerations

Consider the following when using the Export Devices Wizard:

- The **Devices Export Wizard Summary** page displays the number of devices that are exported to the Citrix Virtual Apps and Desktops Delivery Controller. This page displays this information even if devices fail to export. The **Summary** page displays how many device records were created and how many failed. the names of the failed devices can be found in the CDF trace. To export devices that failed earlier, rerun the Devices Export Wizard. Select the same collections. Add them to the existing Citrix Virtual Apps and Desktops catalog, or create a catalog to add them.



- Devices can only be exported to a single Citrix Cloud customer during a single execution of the wizard. If the Citrix Cloud user has multiple cloud customers to manage, and changes occur during the execution of the wizard process, close the wizard and start it again. Use this process to change the Citrix Cloud customer.
- When creating a machine catalog for a physical device using the Export Devices Wizard, the following exception may appear: *Object reference not set to an instance of an object*. To

resolve this issue, use the Machine Creation Wizard in Studio to import the physical devices to the Citrix Virtual Apps and Desktops machine catalog. When you are using Citrix DaaS™ (formerly Citrix Virtual Apps and Desktops service) in Citrix Cloud, the machine catalog appears in the *Initial Zone*. Manually correct the zone of the machine catalog in Studio. This configuration avoids the error *Cannot connect to the PVS server* when adding more devices. To manually move the machine catalog to correct zone:

1. Log into Studio.
2. In the zones node, manually drag the machine catalog to the desired zone.

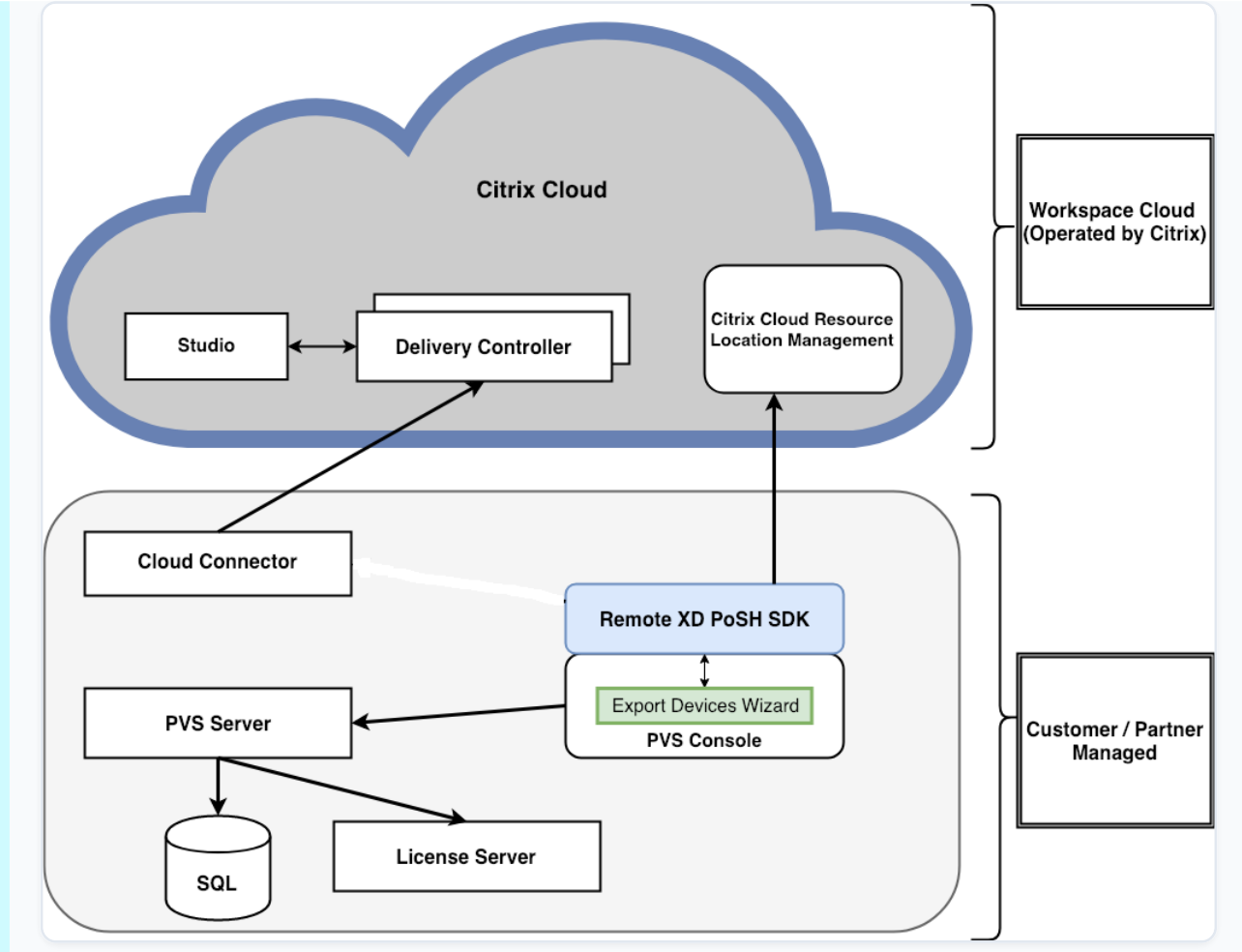
Nutanix limitations

Existing provisioned Nutanix devices cannot be exported to Citrix Cloud because a Nutanix VM MAC address cannot be obtained. This limitation is similar to the behavior of the machine creation wizard in the Citrix Studio. To add a Nutanix device to the Citrix Cloud Delivery Controller, create a device using the Citrix Virtual Apps and Desktop Setup Wizard on Citrix Provisioning console.

Architecture

The following image illustrates elements comprising the Citrix Cloud architecture as part of the Devices Export Wizard functionality.

> **Note:**
>
> The on-premises configuration remains unchanged. The Devices Export Wizard functions with the on-premises Citrix Virtual Apps and Desktops Delivery Controller.



The wizard:

- runs on the Citrix Provisioning console and adds existing provisioned devices to the Citrix Cloud Delivery Controller.
- uses SOAP and MAPI calls to interact with the Citrix Provisioning server to retrieve information on existing provisioned devices.
- interacts with the Citrix Virtual Apps and Desktops remote PowerShell SDK to communicate with the Customer Managed Delivery Controller and the Citrix Cloud Delivery Controller to add provisioned devices to the machine catalog.

Using the devices export wizard

Use the information in this section to install elements required for Devices Export Wizard functionality.

Important:

> For on-premises deployments, the Citrix Virtual Apps and Desktops Delivery Controller is unmodified. No further installation or configuration changes are required. The Citrix Provisioning console installer, version 1912 or later, provides all the necessary components required to use the Export Devices Wizard.

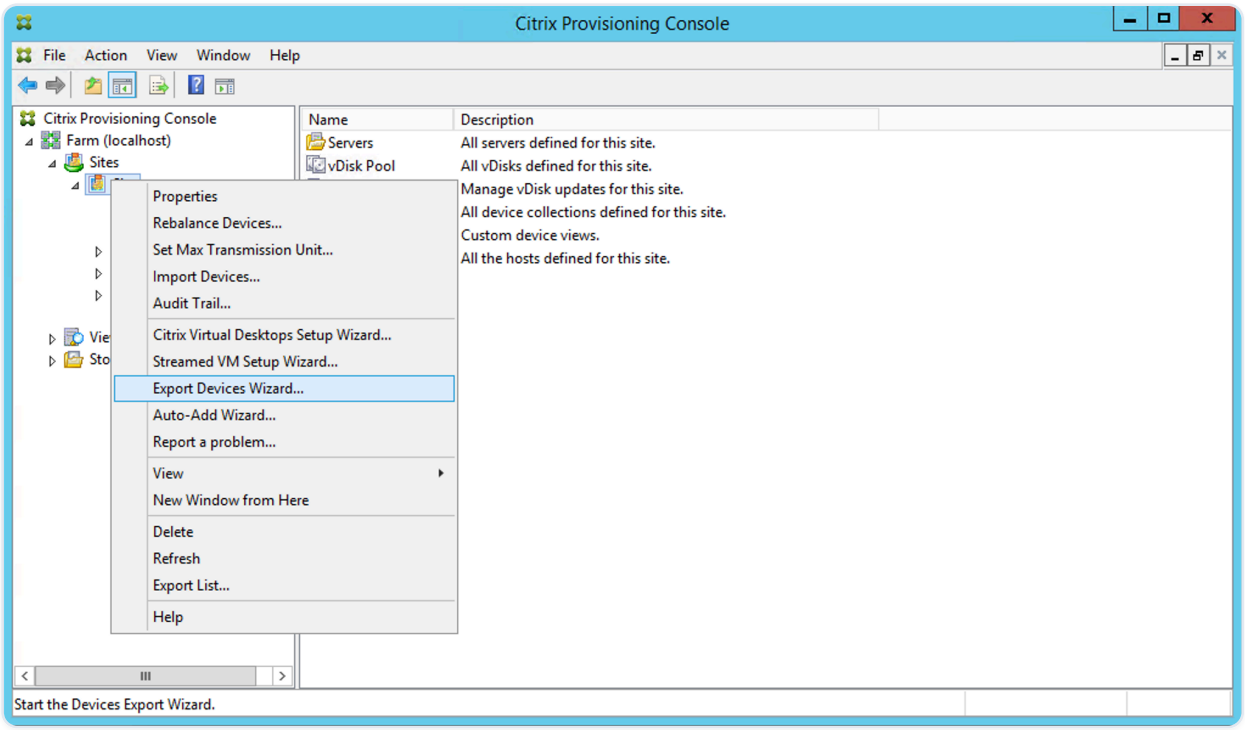
> For Citrix Cloud deployments:

1. Install the Citrix Cloud Connector.
2. Upgrade Citrix Provisioning to version 1912 or later.

For information about provisioning in Citrix Cloud, see Citrix Provisioning managed by Citrix Cloud. For more information about installations related to Citrix Cloud deployments, see Using PVS with the Citrix Cloud Apps and Desktop Service.

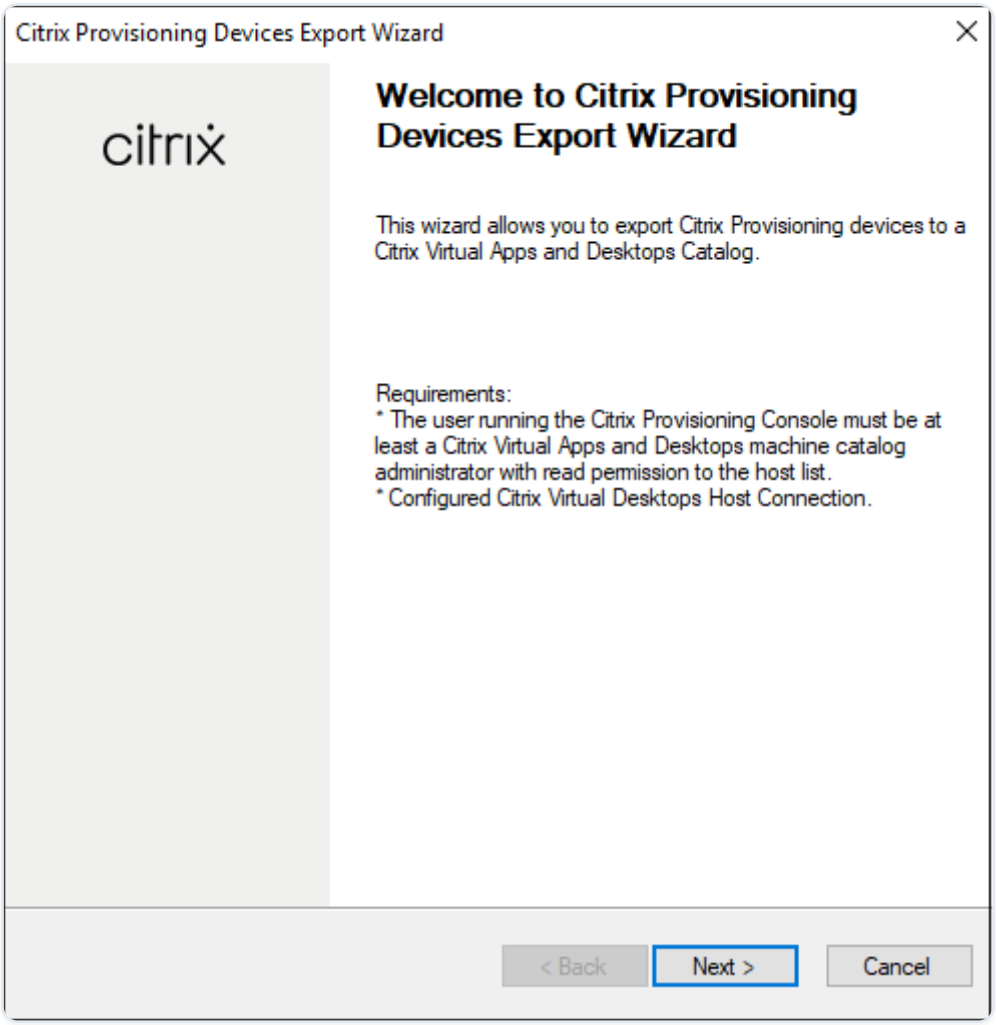
To launch the Devices Export Wizard:

1. In the Citrix Provisioning console, click the **Sites** node.
2. Right-click the Site you want to configure, and right-click to expose a contextual menu.
3. In the context menu, click **Export Devices Wizard**.



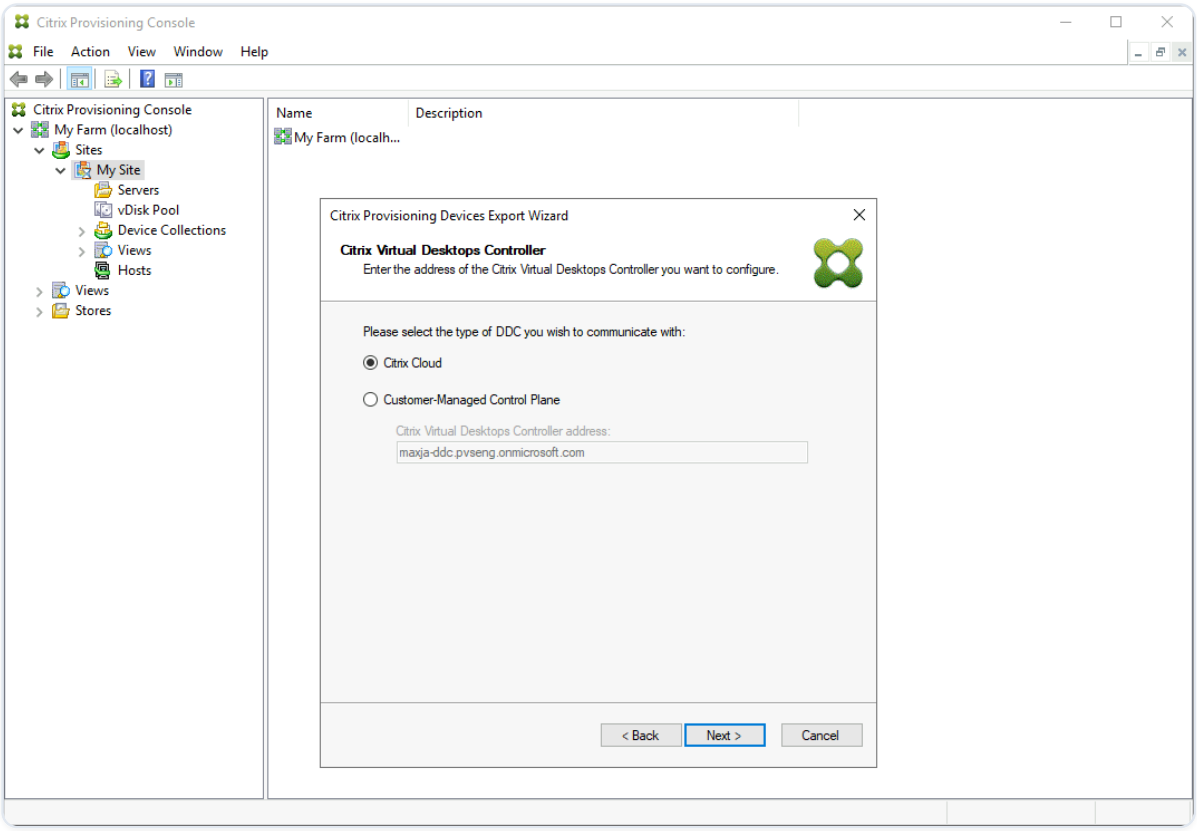
The **Export Devices Wizard** screen appears.

4. Click **Next** to start the wizard.

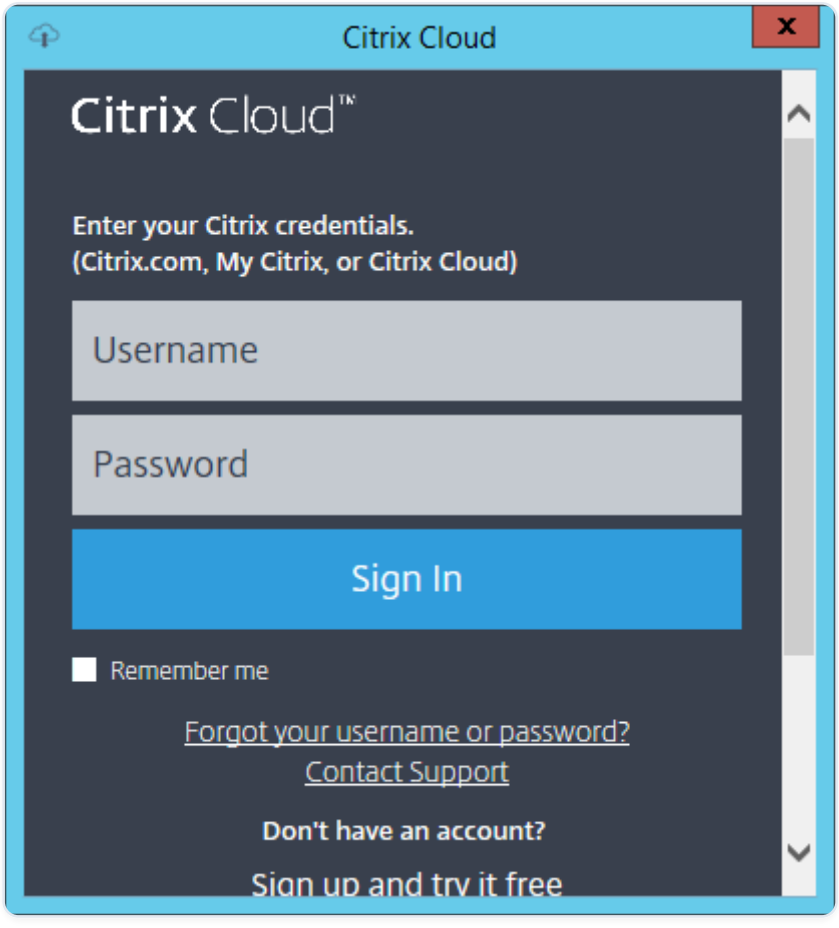


5. On the **Citrix Virtual Desktops™ Controller** screen, select the type of Delivery Controller.

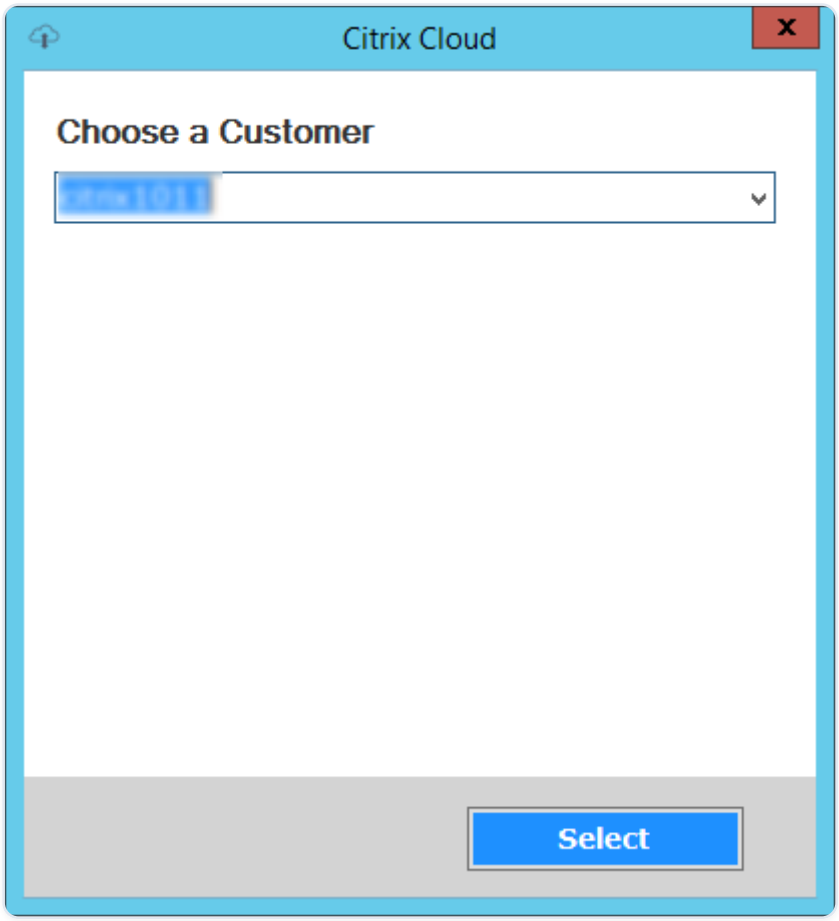
    a. If you select **Citrix Cloud**:



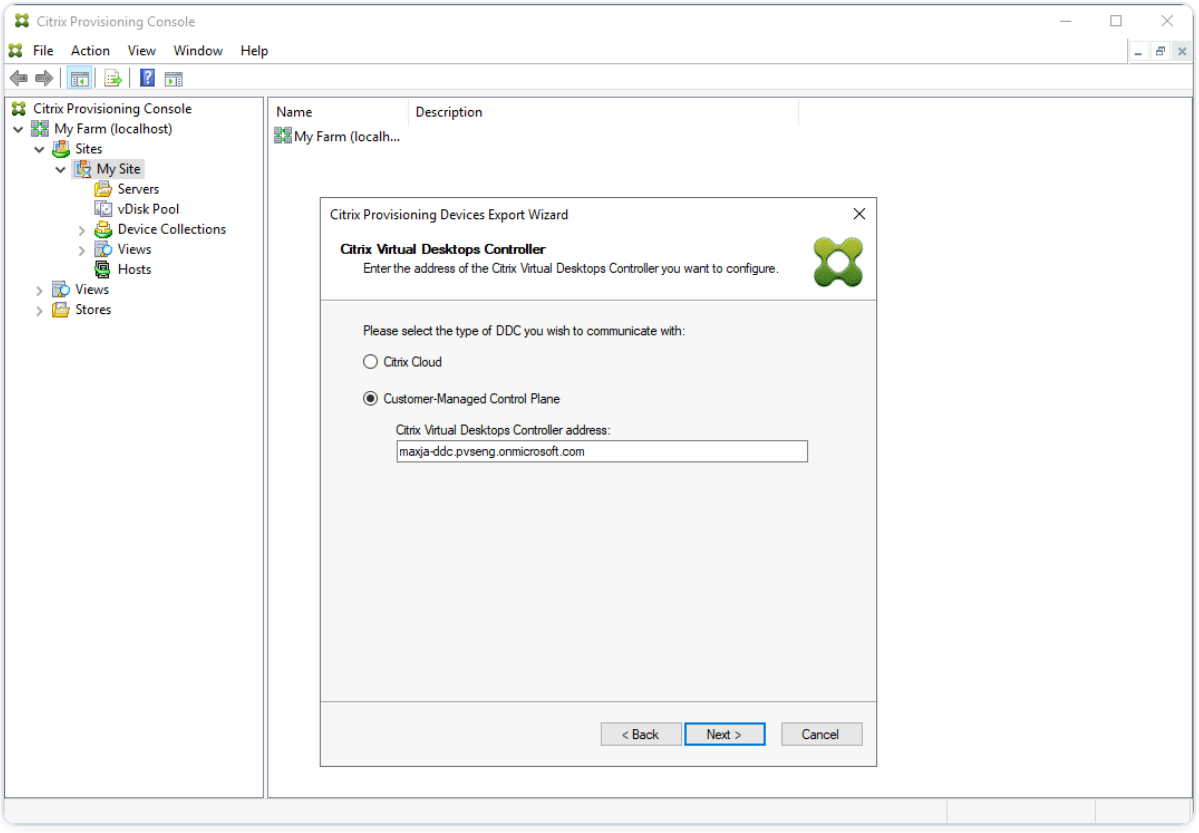
i. Enter your **Citrix Cloud credentials**. Click **Sign In**.



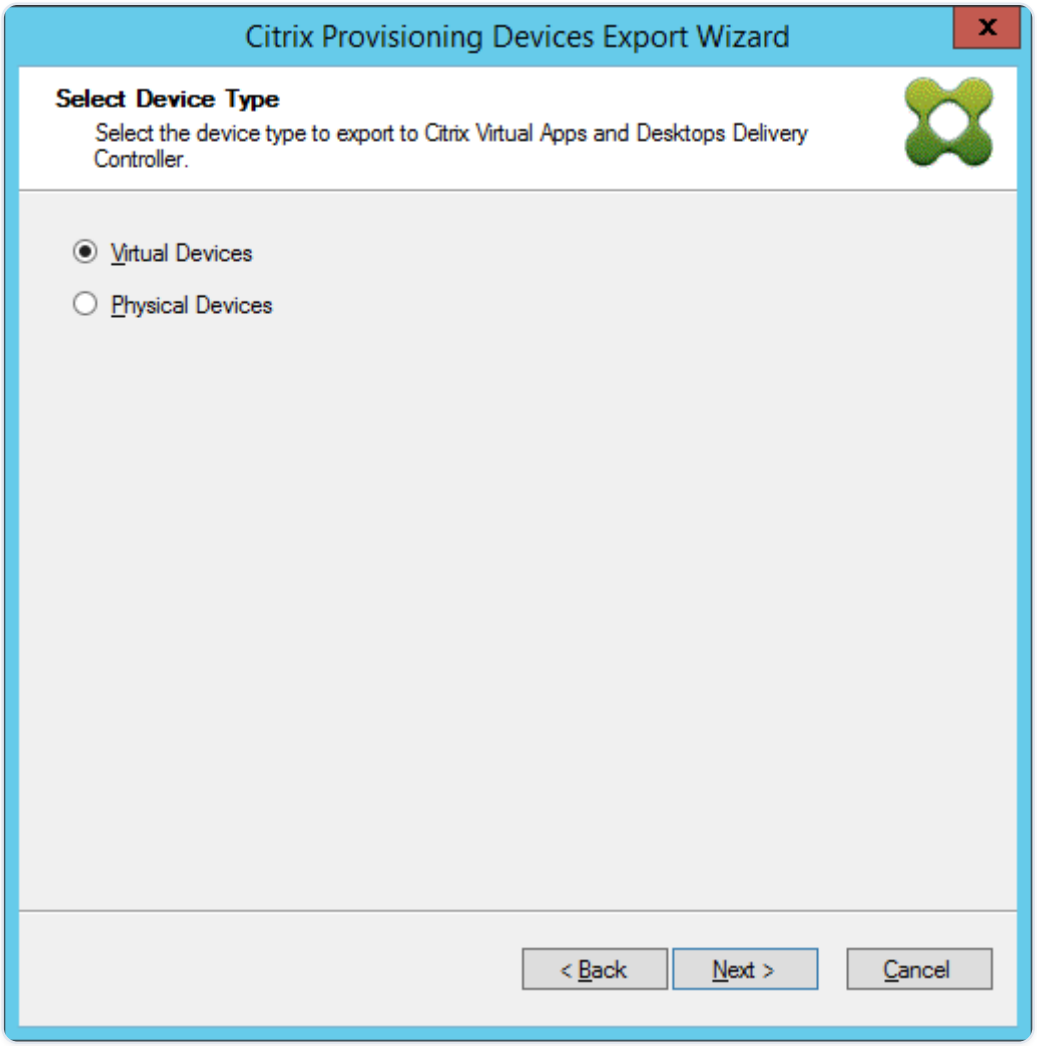
ii. After signing in to Citrix Cloud, select the appropriate cloud customer if requested.



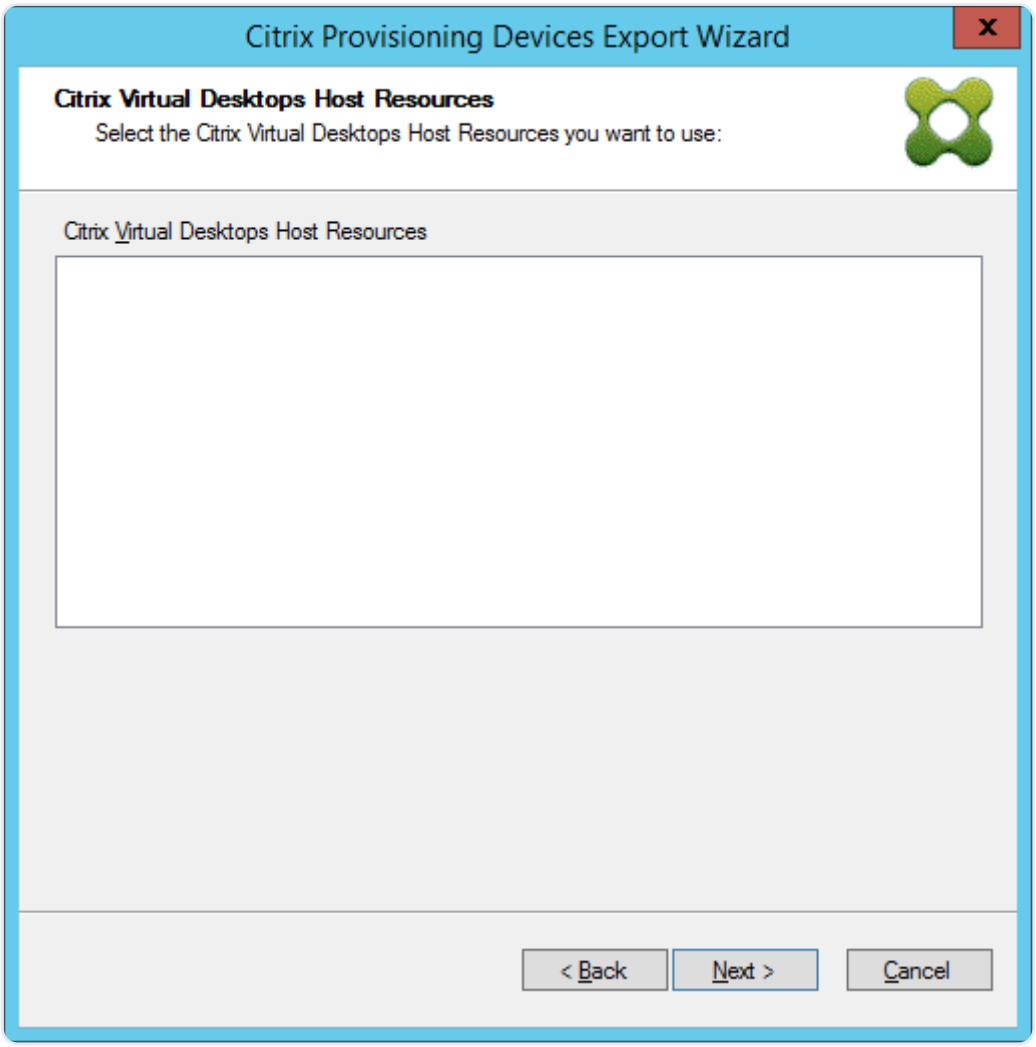
b. If you select **Customer-Managed Control Plane**, enter the controller hostname or address. This will authenticate using your current logged in user.



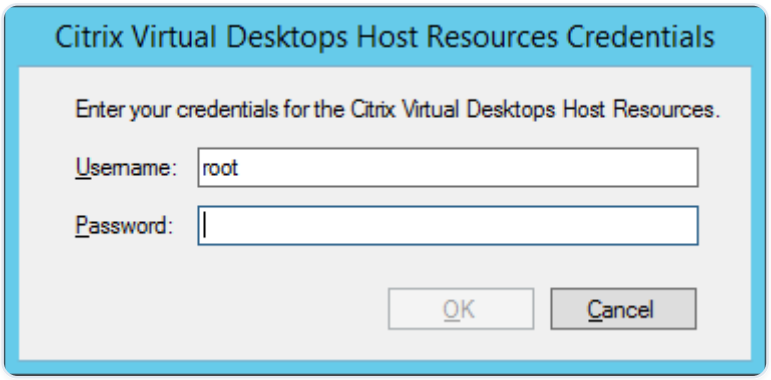
6. Click the **Device Type** to export. Select **Next**. Selecting **Virtual Devices** creates power managed Citrix Virtual Apps and Desktops catalog. Physical devices in the Citrix Virtual Apps and Desktops catalog are unmanaged. When selecting **Virtual Devices**, the wizard displays the **Host Resource** screen which allows you to click the host or hypervisor. For physical devices, the wizard skips to the **Active Directory and Collection** selection screen.



7. Click the host resource. Select **Next**.

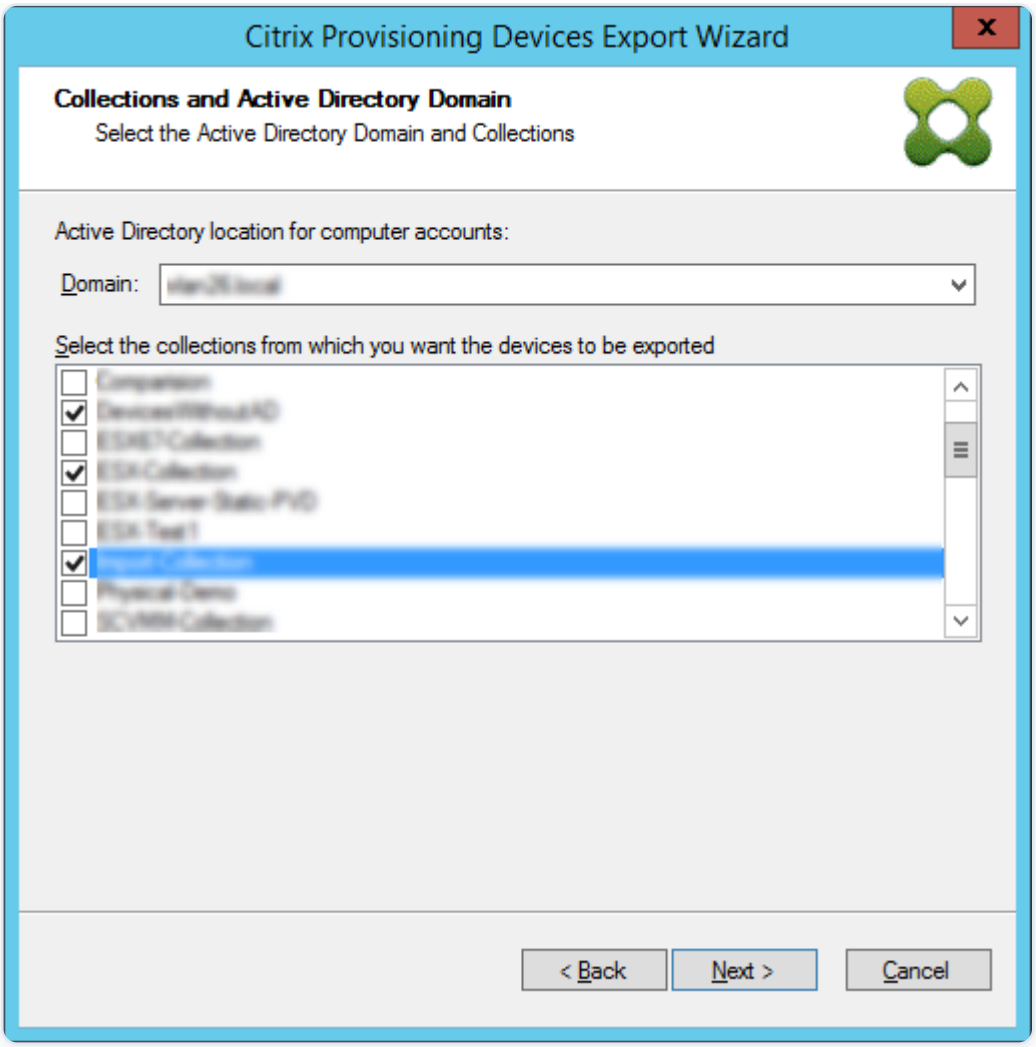


8. When selecting the host resource, you must associate a user name and password. Select **OK**.



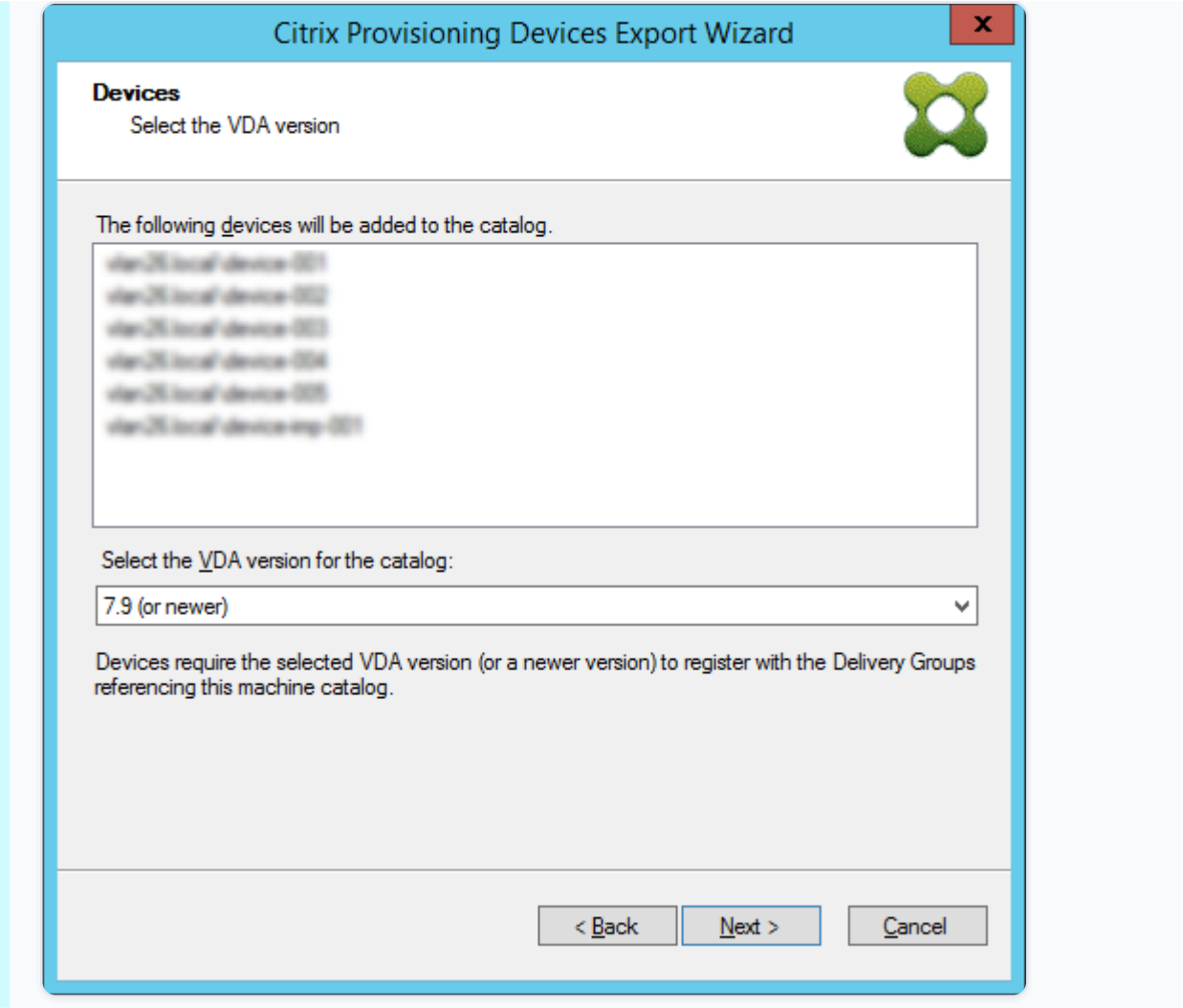
9. Click the Active Directory domain and collections that you want to export. Select **Next**.

> **Note:**
>
> The **Domain** field lists all domains (trusted and untrusted) for selection.

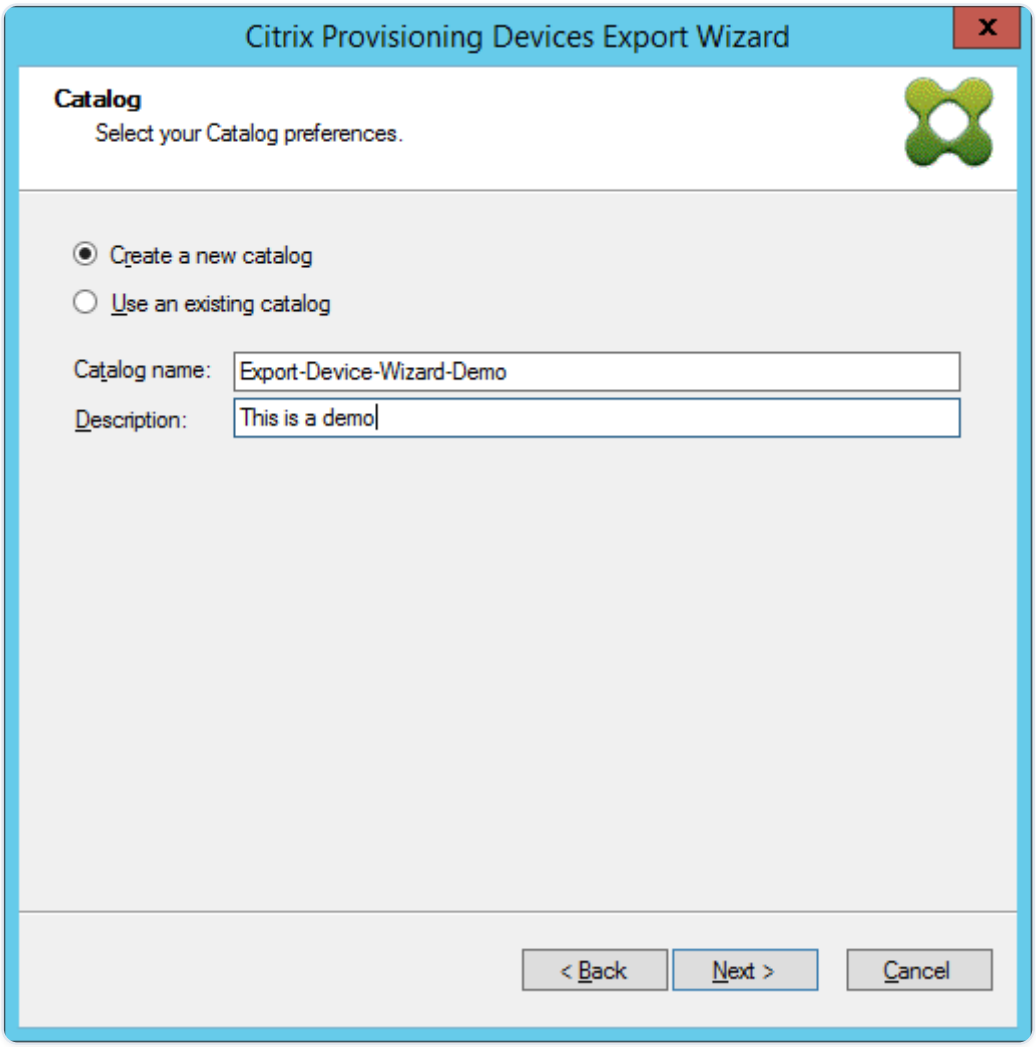


10. Use the list to select the **VDA version**. Devices are required to register with the Delivery Controller referencing the machine catalog. Select **Next**.

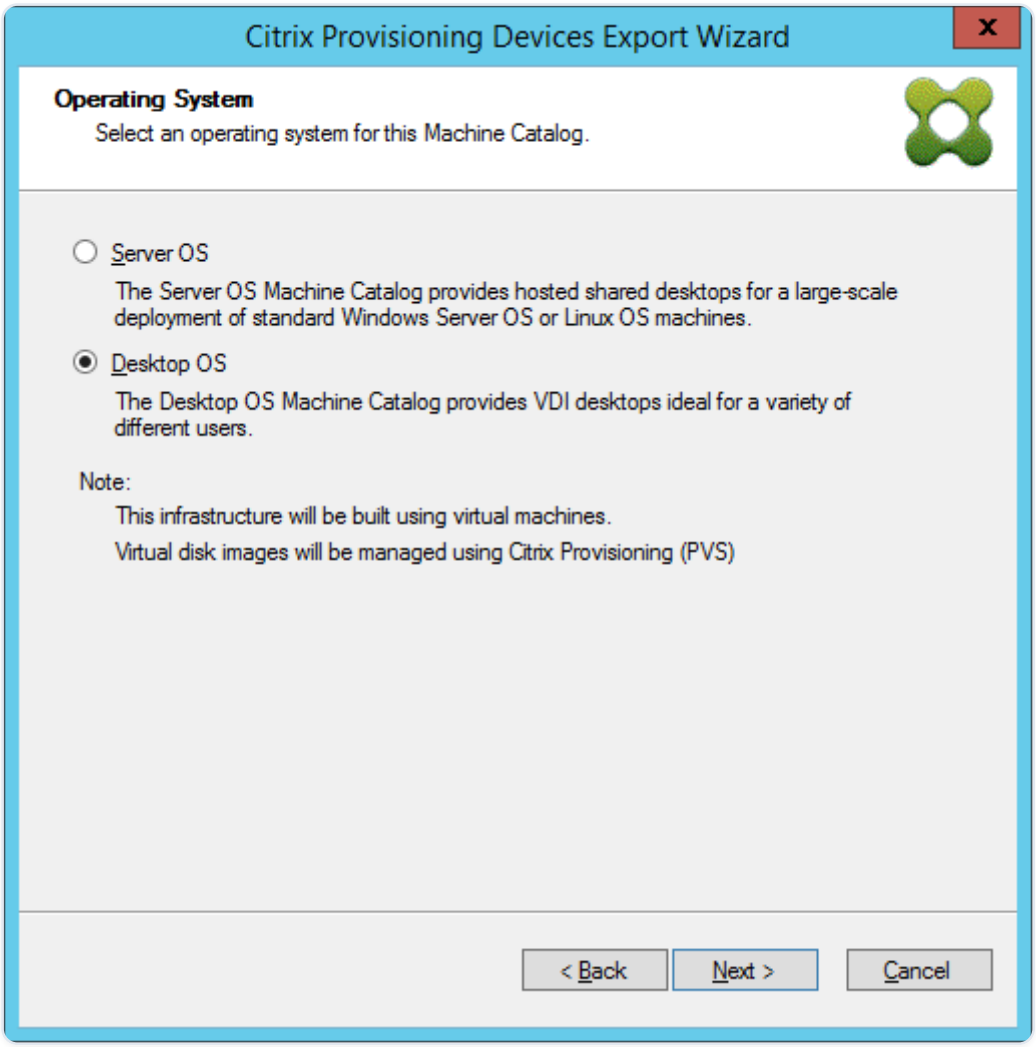
> **Tip:**
>
> All displayed devices are exported to a single Citrix Virtual Apps and Desktop catalog. You cannot select a device in this list.



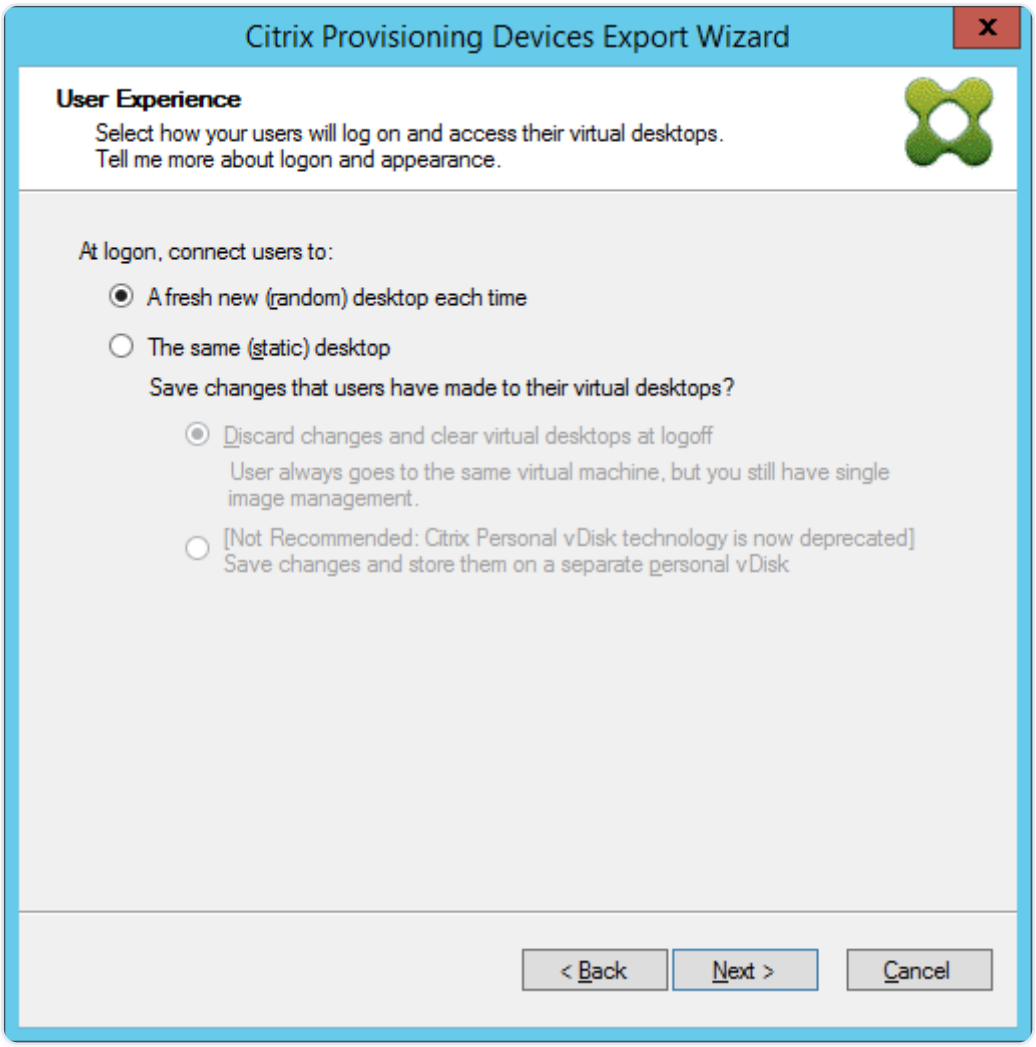
11. Click machine catalog preferences. If you are creating a catalog, specify the name and optionally include a description. Select **Next**.



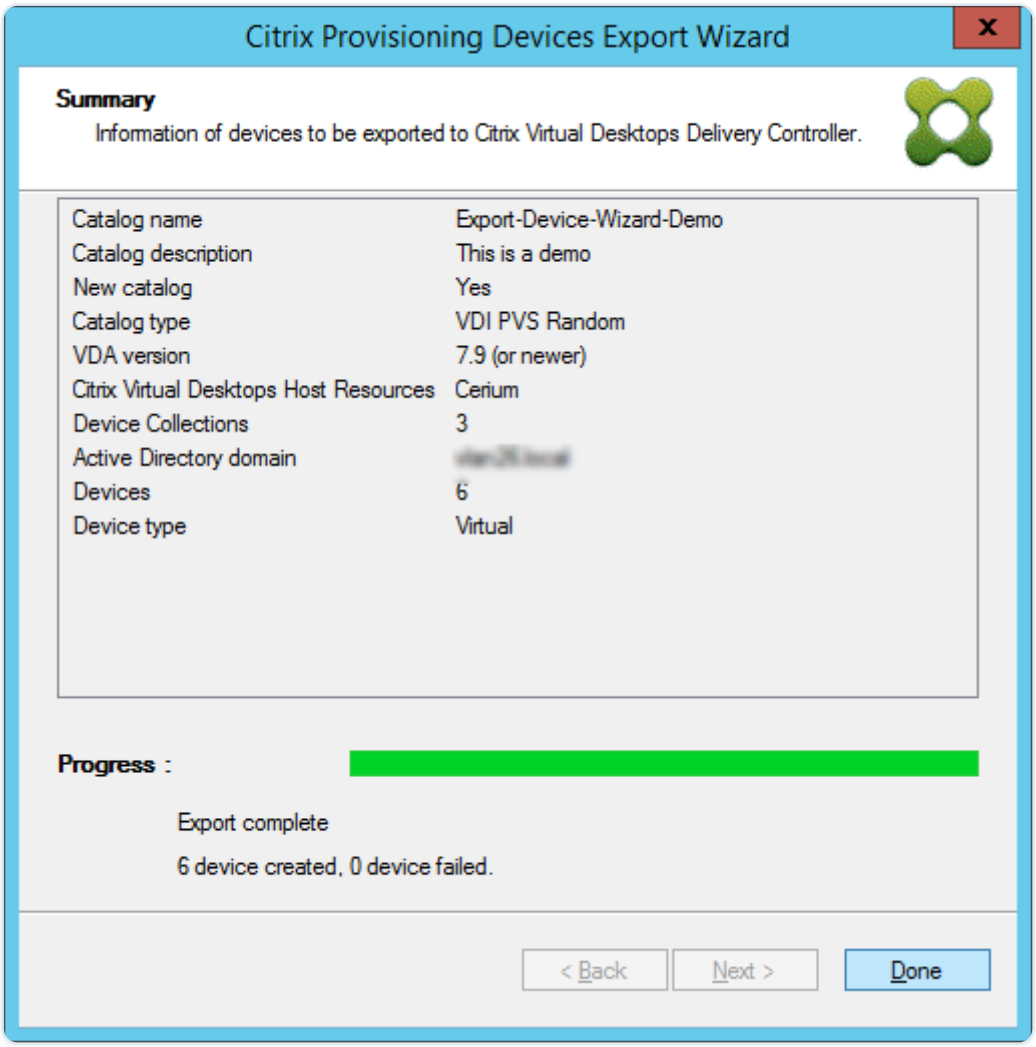
12. Click the operating system. Select **Next**.



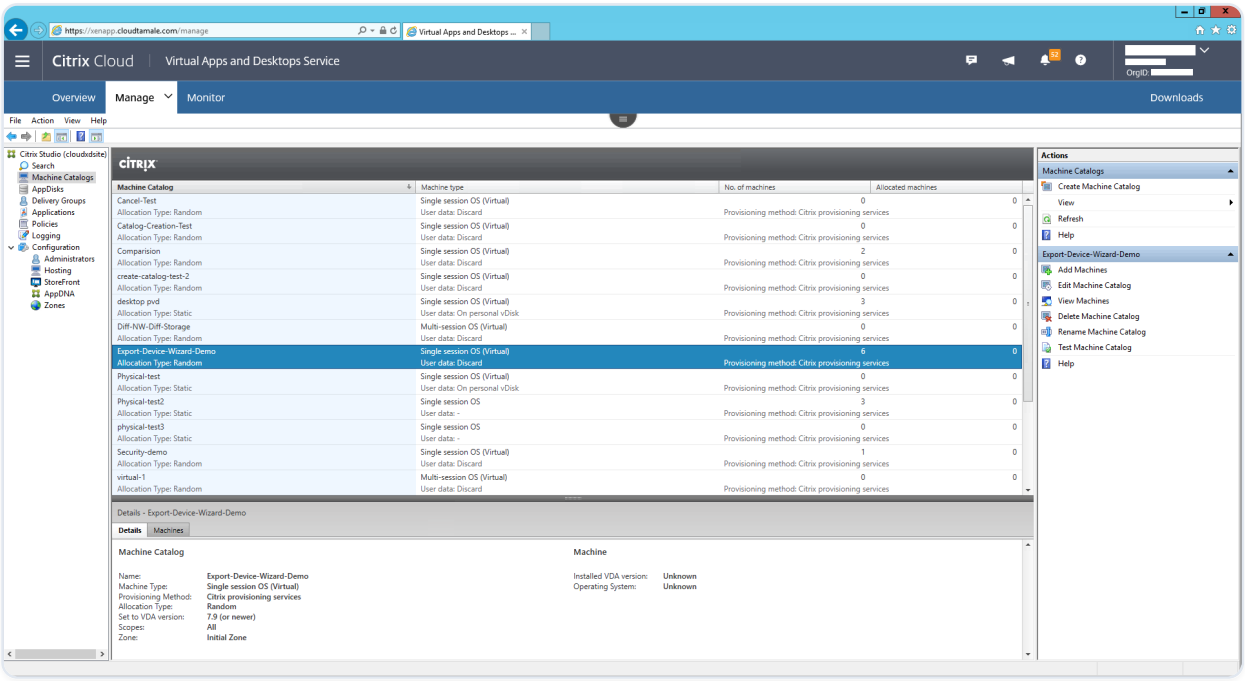
13. Set the user experience for the virtual desktop. Select **Next**.



14. Select **Finish** in the **Summary** screen to complete the wizard process.



Once the wizard finishes, use the Machine Catalog Screen to view the Citrix Virtual Apps and Desktops catalog. Ensure that the catalog was created with the associated machines.



Using the Streamed VM Setup Wizard

The Citrix Provisioning™ Streamed VM Setup Wizard deploys a streamed virtual disk to several cloned virtual machines (VMs).

Use the wizard to:

- Create VMs on a supported hosted hypervisor from an existing template:
  - Citrix Hypervisor™
  - Hyper-V via SCVMM
  - ESX via vCenter
- Create Citrix Provisioning target devices within a collection
- Assign a virtual disk image that is in standard image mode to the VMs

Before running the wizard, be sure that the following prerequisites are met:

- One or more hypervisor hosts exist with a configured template.
- A Device Collection exists in the Citrix Provisioning site.
- A virtual disk in standard image mode exists, associated with the selected VM template.
- Template VM Requirements:
  - Boot order: Network/PXE first in list (as with physical machines).
  - Hard disks: If using local write cache, an NTFS formatted disk large enough for the cache must exist. Otherwise, no hard disks are required.
  - Network: Static MAC addresses. If using Citrix Hypervisor, address cannot be 00-00-00-00-00-00
- The Citrix Provisioning console user account was added to a provisioning site admin group or above.
- When creating accounts in the console, you need permissions to create the Active Directory account. To use an existing one, consider that the Active Directory account must exist in a known OU for selection.
- If you are importing an Active Directory .CSV file, use the following format: `<name>,<type>,<description>`. The .CSV file must contain the column header. For example:

  `Name,Type,Description,`

`PVSPC01,Computer,,`

The trailing comma must be included to signify three values, even if there is no description. This method is the same formatting used by Active Directory Users and Computers MMC when exporting the contents of an organizational unit.

- If you are running a vCenter server on alternate ports, the following registry modifications must be made to connect to it from Citrix Provisioning:
  - Create a new key `HKLM\Software\Citrix\CitrixProvisioning\PlatformEsx`
  - Create a string in the `PlatformEsx` key named `ServerConnectionString` and set it to `http://{0}:PORT#/sdk`

    > **Note:**
    >
    > If you are using port 300, ServerConnectionString= `http://{0}:300/sdk`

This wizard creates VMs, associates Citrix Provisioning target devices to those VMs, and assigns a shared virtual disk to them.

The wizard is run directly from a Citrix Provisioning console.

1. Right-click on the **Site** icon in the **Console** tree panel, then select the **Streamed VM Setup Wizard**...menu option. The **Welcome to the Streamed VM Setup Wizard** dialog appears.
2. Click **Next** to begin the setup.
3. Select the type of hypervisor to connect to, then enter the required connection credentials.
4. Click **Next** to verify the connection.

> **Note:**
>
> For convenience, the most recently used hypervisor and user name are cached in the registry of the local machine running this instance of the provisioning console.

> XenServer 5.5 Update 2 hypervisors are not supported in the 5.6.1 Streamed VM Setup Wizard. System Center Virtual Machine Management (SCVMM) servers require PowerShell 2.0 to be installed.

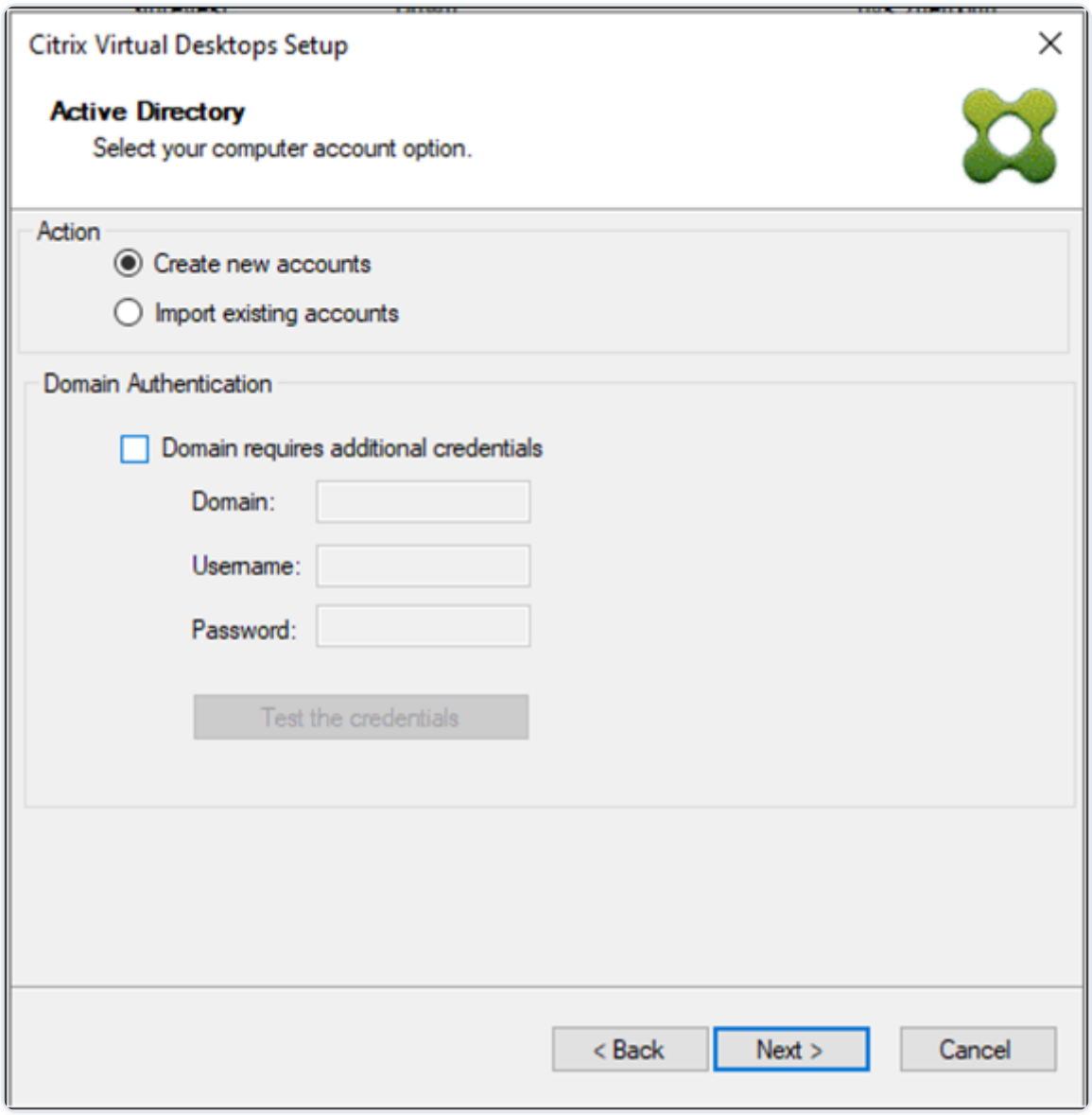
5. Optional. On the **Hypervisor cluster** screen, select the hypervisor host or cluster to host the VMs, then click **Next**.
6. Select one VM template from the specified host, then click **Next**.
7. On the **Collection and vDisk** page, select the collection in which to add VMs.
8. Select a single shared virtual disk within to assign to VMs within that collection, then click **Next**.
9. Set the number of VMs to create, the number of vCPUs, and the amount of Memory used by each new virtual machine.
10. Select the radio button next to one of the following methods, then click **Next**:

    - Create accounts
    - Import existing accounts

    > **Note:**
    >
    > The Active Directory administrator must delegate rights to the Citrix Provisioning console user to allow Active Directory account creation.
    >
    > The domain and OU default to those rights of the current user.
    >
    > New computer names that are created are first validated that they do not exist as computers in Active Directory, VMs, or target devices.
    >
    > Citrix Provisioning supports provisioning of target devices in untrusted domains.

    If the domain is not trusted, under **Domain Authentication**, do the following:

    a. Select **Domain requires additional credentials**.
    b. Enter the domain name, username, and password for the untrusted domain.
    c. Click **Test the credentials**. This action validates the domain name and the credentials.
    d. After you get a green check mark, proceed to the next page.



11. If the **Create new accounts** method is selected:

    - Click **Next**. The Active Directory accounts and location screen appears.
    - Select the appropriate domain from the **Domain** menu, then select from the OUs listed for that Domain.
    - In the **Account naming scheme** menu, select a valid naming scheme consisting of at least one hash symbol (#) that is 15 characters or less. Also, select a number/character fill option that dynamically replaces the hash symbols in the specified naming scheme, incrementing by one for each VM as they are created.

    If **Import existing accounts** is selected:

    - Click **Next**. The Active Directory accounts and location page appears.
    - Click **Browse** to browse for an Active Directory Organizational Unit to import Active Directory account names, or click **Import** to import account names from a CSV file.

Note:

The Required count displays the number of virtual machines previously specified to be created. The **Added count** displays the number of validated entries added to the list.

12. Review all configuration settings, and then click **Next** to confirm and finish configurations.

Note:

Clicking **Cancel** cancels the configuration of any additional machines, and the quantity of successfully configured machines displays under the Progress bar. Progress is retained if the wizard fails or is canceled in the middle of an operation. Cleanup existing progress manually, which includes removing the following:

- Citrix Provisioning target devices created in the selected collection.
- VMs created in any of the selected hosts hypervisors.
- Active Directory computer accounts that were created.

Important:

When using the setup wizard to specify names associated with storage devices, do not use a comma. Citrix Virtual Apps and Desktops™ retains names associated with storage devices, separated by commas. For example, Storage 1, Storage 2, Storage 3. If a storage name includes a comma, for instance, `Storage1,East`, Citrix Provisioning erroneously recognizes it as two separate storage devices.

Tip:

There is a risk that moving target devices from site to site might cause them to be deleted in the future. This risk increases if the target device was created using the Streamed VM Setup Wizard. Citrix® recommends that you avoid moving target devices from site to site.

Deploying virtual desktops to VMs using the Citrix Virtual Apps and Desktops™ Setup Wizard

The Citrix Virtual Desktops™ Setup Wizard helps with deploying virtual desktops to virtual machines (VMs).

> **Important:**
>
> - The Citrix Provisioning server must have direct access to the storage device to facilitate communication. The provisioning user must have read\write access to the storage device to ensure successful provisioning with the HDD BDM.
> - Currently, you cannot create target VMs using HDD BDM boot if you install Citrix Provisioning™ Servers on the system running Windows Server Core.

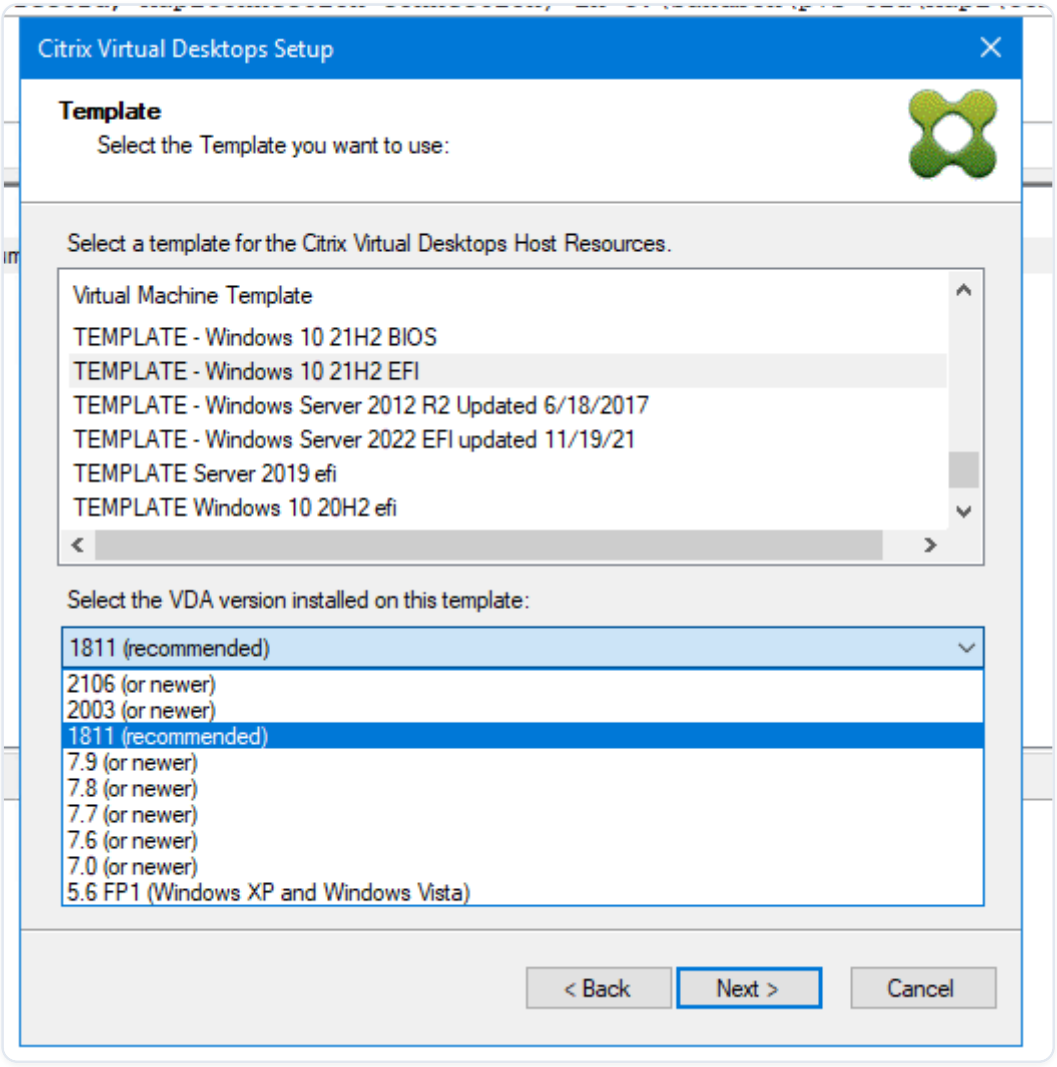
The wizard:

- Creates VMs on a Citrix Virtual Apps™ and Desktops-hosted hypervisor using an existing machine template:
  - XenServer (formerly Citrix Hypervisor™)
  - ESX through vCenter
  - Hyper-V using SCVMM. When provisioning to an SCVMM server, the wizard automatically changes the network configuration of both the first legacy NIC and the second synthetic NIC for Gen 1 VMs. See the **SCVMM** section for more information.
  - Nutanix Acropolis (from snapshots). See Nutanix Acropolis requirements for more information.
- Creates Citrix Provisioning target devices within a new or existing provisioning device collection matching the Citrix Virtual Apps and Desktops catalog name.
- Creates Hybrid Azure AD joined catalogs. For information, see Create Hybrid Azure AD joined catalogs.
- Assigns a Standard Image virtual disk to VMs within the device collection.
- Adds the target to the selected Active Directory OU.
- Adds virtual desktops to a Citrix Virtual Apps and Desktops catalog.

Important considerations

Consider the following when using the Citrix Virtual Apps and Desktops Setup Wizard:

- For Citrix Virtual Desktops Setup Wizard provisioned Gen 2 VMs, the BDM partition is FAT formatted with a drive letter. As a result, Windows in a Citrix Provisioning private image are aware of the new partition. For example, an RDS provisioning image using a write cache disk and BDM partition has 2 partitions in private image mode.
- When using the Linux streaming feature, consider that a new step was added to the Citrix Virtual Apps and Desktops Setup Wizard. Add the SOAP SSL certificate to ensure that the Linux target can image the virtual disk through the SOAP server. For details, see Installation.
- Using the Citrix Provisioning Setup Wizard to create VMs on a XenServer host while specifying 1 vCPU, creates a VM with 1 vCPU. However, the topology possesses 2 cores per socket. Creating VMs in this fashion prevents the VM from booting, while displaying the following error message in XenCenter: `The value 'VCPU\_max must be a multiple of this field` is invalid for field `platforms:cores-per-socket`. As a result, XenCenter fails to boot the VM because the topology and vCPU configuration are incompatible.
- The Citrix Virtual Apps and Desktop Setup Wizard creates targets then boots them to format the cache drive. This process occurs quickly. A VDA occasionally reaches a state where it fails to shut down correctly. This process occurs because the VDA is initializing while the Citrix Provisioning Device Service simultaneously finishes formatting the cache drive then shuts down the target. To resolve this issue, in the virtual disk registry key, HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CitrixProvisioning, create a DWORD called "RebootDelaySec". Set an arbitrary value, delay-to-shutdown, in seconds using a decimal value.
- When using the Citrix Virtual Apps and Desktops Setup Wizard, the default VDA level is the same as that used in Studio.



About Citrix Studio tools

When using Citrix Studio to create provisioned catalogs, consider:

- The Citrix Virtual Apps and Desktops Setup Wizard provisions target VMs and adds them to a broker catalog.
- The Export Devices Wizard adds existing provisioned target VMs to a broker catalog.

With both wizards, authentication occurs to Citrix Virtual Apps and Desktops. Hosting connections are retrieved so that you can select the connection used by the broker to power manage the provisioned target VMs.

> **Tip:**
>
> Only *hosting units*, not *hosting connections*, can be used. These hosting units are only created when you specify **Studio Tools** when the hosting connection is created.

ESX permissions

For ESX, the minimum permissions include the following:

- Datastore Permissions
  - Allocate space
  - Browse datastore
  - Low level file operations
- Network Permissions
  - Assign network
- Resource Permissions
  - Assign virtual machine to resource pool
- System Permissions - These permissions are automatically added when you create a role in vCenter.
  - Anonymous
  - Read
  - View
- Task Permissions
  - Create Task
- Virtual machine configuration Permissions
  - Add existing disk
  - Add new disk
  - Advanced
  - Change CPU count
  - Change resource
  - Memory
  - Modify device settings
  - Remove disk
  - Settings

- Virtual Machine/Interaction
  - Power Off
  - Power On
  - Reset
  - Suspend
- Virtual Machine/Inventory
  - Create New
  - Create from existing
  - Remove
  - Register
- Virtual Machine/Provisioning
  - Clone virtual machine
  - Clone template
  - Allow disk access
  - Allow virtual machine download
  - Allow virtual machine files upload
  - Deploy template
- Global
  - Manager custom attributes
  - Set custom attribute

Write cache considerations

The Citrix Virtual Apps and Desktops setup Wizard discards any hard disks that are attached to a template. This process minimizes provisioning time.

The wizard provisions diskless VMs if the virtual disk is in standard image mode and cache is set as cache on the server. If the cache is server-side, Citrix Provisioning does not automatically boot the provisioned VMs.

The wizard provisions VMs with write cache drives (the default size is 6 GB and the default type is dynamic). If the virtual disk is in standard image mode and cache is set as cache on the local hard disk. To format the write cache drive, the wizard automatically boots the VMs in standard image mode with the cache on the server. After formatting completes, VMs are automatically shut down, then Citrix Virtual Apps and Desktops can boot the VMs as necessary.

If the write cache is stored on hypervisor local storage, configuring deployment through the Citrix Virtual Apps and Desktops Setup wizard varies depending on your hypervisor.

On ESX and Hyper-v, you cannot use the Citrix Virtual Apps and Desktops Setup Wizard to provision VMs if you are using hypervisor local storage.

> **Important:**
>
> When specifying names associated with storage devices, do not use a comma (,). Citrix Virtual Apps and Desktops retains names associated with storage devices separated by commas. For example, Storage 1, Storage 2, Storage 3. If a storage name includes a comma, for instance, `Storage1,East`, Citrix Provisioning erroneously recognizes this format as two separate storage devices.

Limitation

The registry key `UseTemplatecache` created on the Provisioning Server running the Citrix Virtual Apps and Desktops Setup Wizard supports only PXE or ISO mode and not HDD BDM boot.

Virtual disk types

VMs provisioned through the Citrix Virtual Apps and Desktops Setup Wizard have new disks created and attached for local provisioning write cache use. The default virtual disk types created are:

- "Fixed" or "dynamic" depending upon the storage repository used in Citrix Hypervisors
- "Dynamic" for SCVMM 2012 SP1
- "Fixed" for SCVMM 2012
- "Thin-provisioned" for ESX

There is a registry key to override the default types of write cache disks created by provisioning deployments on SCVMM and ESX. This registry key does not apply to XenServer. To force "fixed" (or "eager-zeroed thick" for ESX):

```
[HKEY_CURRENT_USER\Software\Citrix\ProvisioningServices\VdiWizard]
```

```
"OVERRIDE_VM_WRITE_CACHE_DISK_TO_FIXED"="true"
```

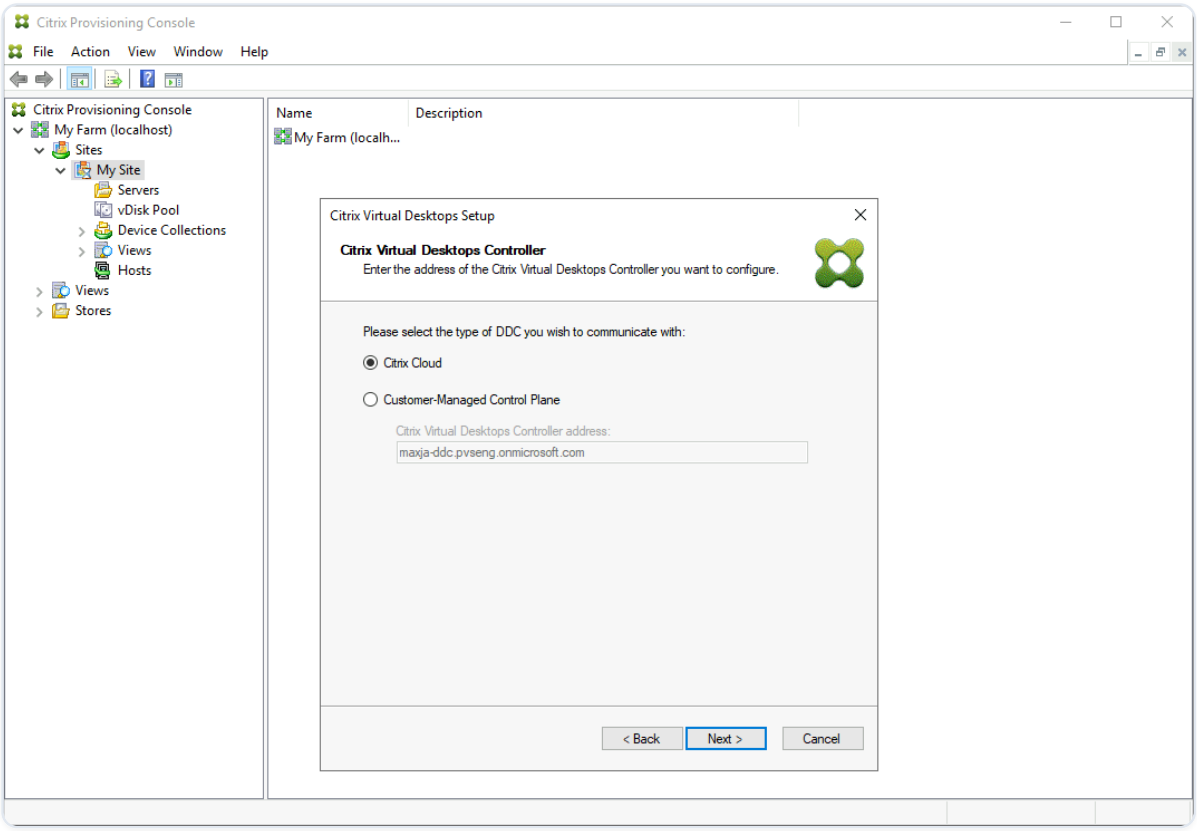
Setting this same key to `false` overrides to the dynamic setting. Remove the key to return to default behavior.

Run the wizard

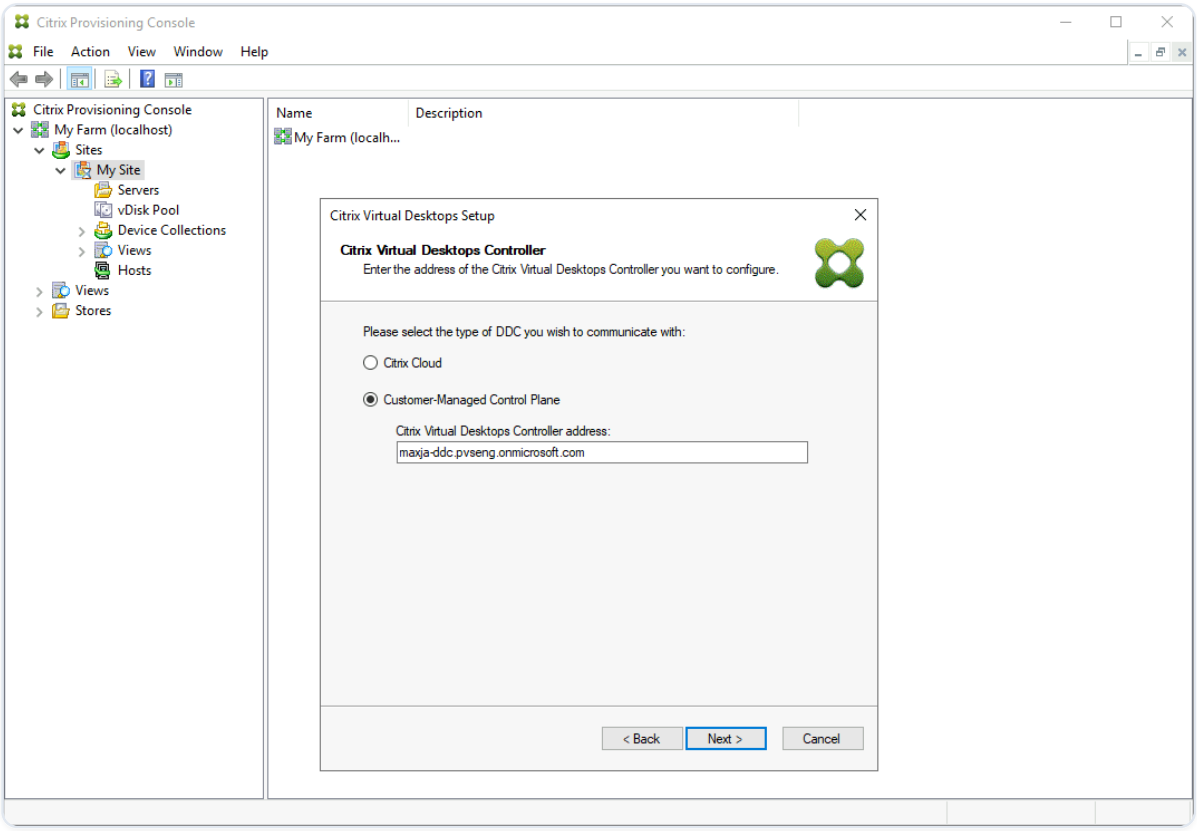
Run the wizard directly from the Citrix Provisioning console or from a remote console.

> **Important:**
>
> - If you are using ISO BDM boot, ensure that the template has the BDM ISO attached to it. Configure the PXE boot option in the **Boot mode in the Virtual Machines** page of the Citrix Virtual Apps and Desktops Setup Wizard.
> - If you want to stream targets over IPv6, ensure that the master target device acquire IPV6 address before capturing the vDisk.

1. Right-click on any Site icon in the **Console** tree panel, then select the **Citrix Virtual Desktops Setup Wizard**...menu option. The Citrix Virtual Desktops Setup Wizard appears. **Note:** The Citrix Virtual Apps and Desktop Setup Wizard is shown as the *Citrix Virtual Desktops Setup Wizard* in the provisioning console.
2. Click **Next** to begin setup.
3. On the **Citrix Virtual Desktops Controller** page, select the type the Delivery Controller.
    a. If you select **Citrix Cloud™**, enter Citrix Cloud Credentials when prompted, and select the cloud customer if requested.



b. If you select **Customer-Managed Control Plane**, enter the controller hostname or address. The wizard authenticates to the Delivery Controller using the current logged in user.



4. On the **Citrix Virtual Desktops Host Resources page**, select a **Citrix Virtual Apps and Desktops host**. If you choose a cluster, machines are evenly distributed across the hosts cluster.

   > **Note:**
   >
   > XenServer 5.5 Update 2 virtualization settings do not display. These settings are added in Citrix Virtual Apps and Desktops as host connections using the **Manually create VMs** option. As a result, you cannot specify a network or storage location for them, therefore it is not listed in the Citrix Virtual Apps and Desktops Setup Wizard.

5. Supply the host credentials, user name, and password.
6. On the **Template** page, from the list of available templates, select the template to use for the host you chose. If using a previous version of the VDA or if the template is built using Windows Vista, select the check box. Valid templates must have a dynamic MAC address or a static address with a value (00:00:00:00:00:00 is not a valid MAC address).
7. If there is more than one network available for the **Virtualizations Settings**, the **Network** page displays so you can select the appropriate network.
8. On the **vDisk** page, select a single standard image mode virtual disk to assign to the collection of VMs.
9. Create a catalog or use an existing catalog from a previous release (Vista or Windows 7 with VDA 5.6). The options available depend on which catalog option you select:

   - If you chose to create a catalog, provide a name and description for that catalog. Appropriate machine types include:
     - Windows Client Operating System – best for delivering personalized desktops to users, or delivering applications to users from desktop operating systems.
     - Windows Server Operating System – best for delivering hosted shared desktops for large scale deployment of standardized machines or applications, or both.
     - The vGPU option is only supported on desktop operating systems.
   - If you select an existing catalog using the menu, that catalog's description, machine type, assignment type, and user data appear.

10. On the **Virtual machines** page, select **VM preferences**. Preferences vary depending on the machine OS type and if assigned user changes are discarded after the session ends.

a. For Windows Client or Windows Server machines that are randomly assigned to users:

- Enter the number of VMs to create (default is 1)
- Enter the number of vCPUs (default is based on the previously selected template)
- Enter the memory size. If the template has dynamic memory configured, two extra configuration settings are required (minimum and maximum memory)
- Enter the local write cache disk size (default is 6 GB)
- Select the checkbox **Targets uses IPv6** if you want to create targets that stream using IPv6.
- Select a boot mode. PXE boot (requires a running PXE service) and BDM disk (creates a partition for the Boot Device Manager file). You must select the BDM disk option if you want to create targets that stream using IPv6.

11. On the **Active Directory** page, choose the appropriate method for adding Active Directory computer accounts:

- **Create new accounts**
- **Import existing accounts**

The page that displays depends on which Active Directory method you select.

Citrix Provisioning supports provisioning of target devices in untrusted domains.

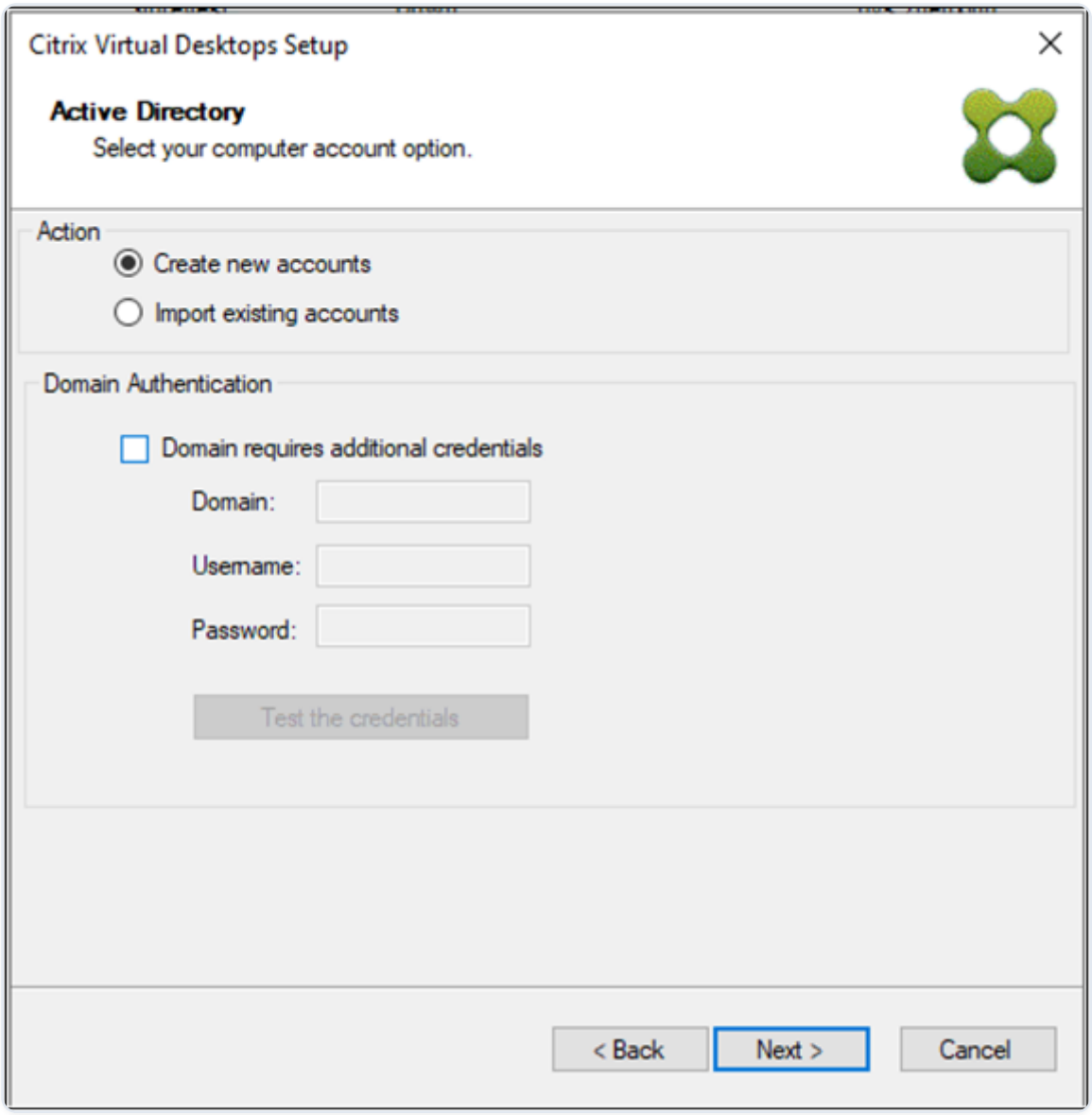
If the domain is not trusted, under **Domain Authentication**, do the following:

a. Select **Domain requires additional credentials**.

b. Enter the domain name, username, and password for the untrusted domain.

c. Click **Test the credentials**. This action validates the domain name and the credentials.

d. After you get a green check mark, proceed to the next page.



12. Follow the instructions depending on whether you want to create AD accounts or import existing AD accounts.

    - If you want to create Active Directory computer accounts:

        a. Select **Create new accounts** on the **Active Directory** page.

        b. Delegate rights to the provisioning console user to allow Active Directory account creation or modification to manage computer account passwords.

        c. Select the appropriate domain from the **Domain** menu box, then select from the OUs listed for that domain. The domain and OU default to rights of the current user.

        d. Select the machine-naming option from the **Account naming scheme** menu text box. Enter a valid naming scheme consisting of at least one hash symbol (#) that is 15 characters or less. Also, select a number/character fill option that dynamically replaces

the hash symbols in the specified naming scheme, incrementing by one for each VM as they are created.

- If you want to import existing Active Directory computer accounts:

  a. Select **Import existing accounts** on the **Active Directory** page.

  b. Click **Browse** to browse for the appropriate OU to import, or click **Import** to import an existing `.csv` file in the following format:

  ```
  Name,Type,Description,
  ```

  ```
  PVSPC01,Computer,,
  ```

  The **Required count** displays the number of VMs previously specified and the **Added count** displays the number of entries in the list.

  If you import machine account names that exist in any of the following locations, they are not valid:

  - Citrix Virtual Apps and Desktops (as a machine)
  - Citrix Provisioning (as a device)
  - Hypervisor (as a VM)

  c. If the AD structure contains many objects or containers, or if you are importing many machine accounts, the import might take a long time.

13. For UEFI targets if you select the **BDM boot** mode on the **Virtual machines** page, then you can see the **Citrix Provisioning server information** page. Using this page, set up the information about the provisioning servers that function as login servers for the target devices. You can select:

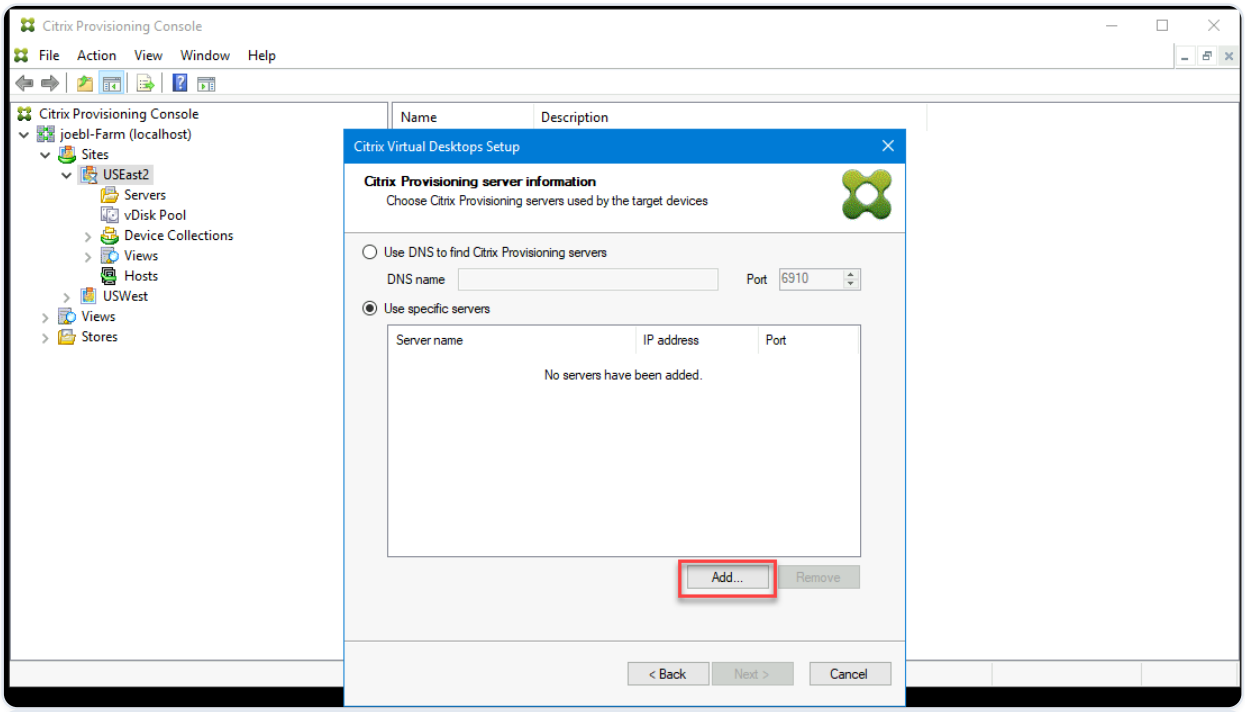
- **Use DNS to find Citrix Provisioning Servers**: If you have one single Citrix Provisioning Server, then you can use its DNS hostname. If you want a single DNS name to translate to multiple PVS servers, then you have to manually add the records with the common name and the IPv4 or IPv6 address of each server.

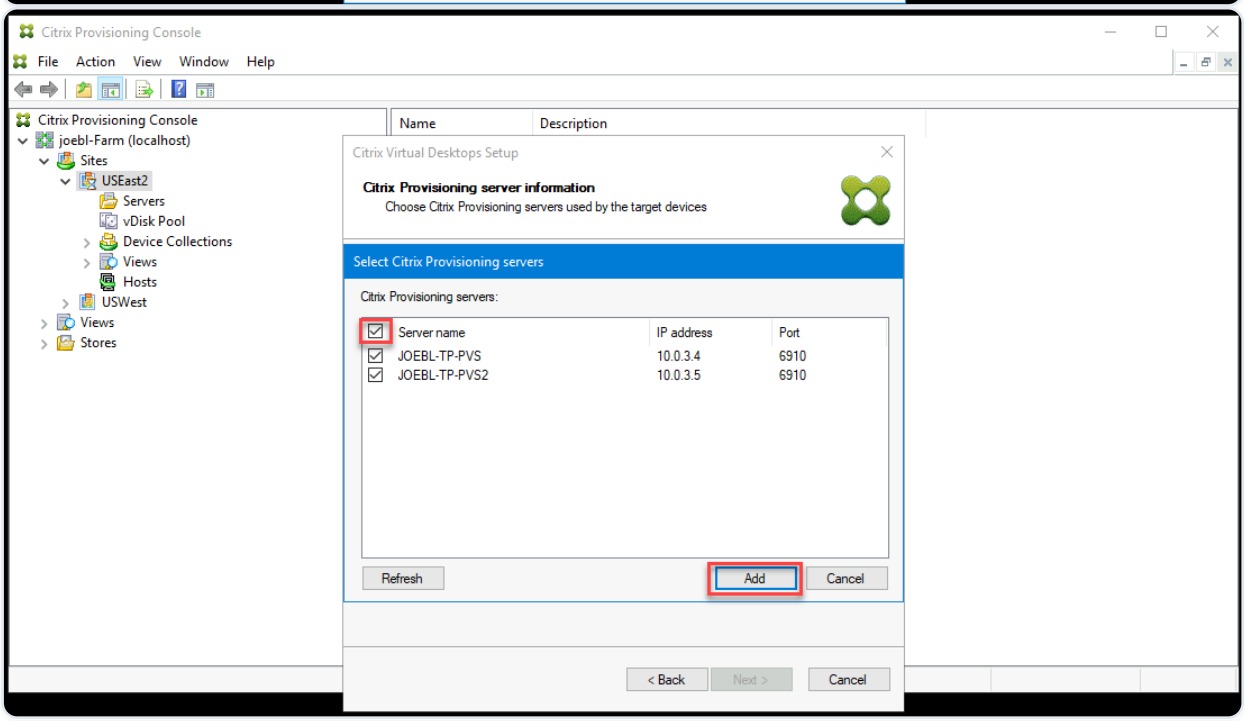
> **Note:**

> If you want to use a DNS name, then you must specify the fully qualified domain name. DHCP server does not include the zone where you add the DNS name to be used.

- **Use specific servers**: To specify the desired servers by IP address, click **Add** to select from the list of configured servers. Select the servers and click **Add**. The selected servers appear on the **Citrix Provisioning server information** page.

> **Note:**
>
> The IPv6 addresses are displayed if you select **Targets uses IPv6** checkbox earlier on the **Virtual Machines** page.





14. Review all configuration settings. After confirming, the following actions take place one at a time across all hosts until configurations are complete:

    - If applicable, create a Citrix Virtual Apps and Desktops catalog
    - Create VMs on a host's hypervisor using the machine template
    - Create BDM partitions, if specified
    - Create a write cache disk of the specified size
    - Create Citrix Provisioning target devices then assign the selected virtual disk to those devices

- Add the target devices to the selected provisioning collection
- Add the VMs to the Citrix Virtual Apps and Desktops catalog
- Boot each VM to format the newly created write cache disk

If you cancel during the configuration, you must manually remove the following:

- Citrix Virtual Apps and Desktops machines from the assigned catalog
- Active Directory computer accounts that were created.
- Newly created Citrix Virtual Apps and Desktops catalogs.
- Citrix Provisioning target devices created in the selected device collection.
- VMs created on any of the selected host hypervisors.

To update and reassign a virtual disk, copy the target device's currently assigned base virtual disk image. Update the image to include new Citrix Provisioning software and drivers. Reassign the updated virtual disk to the target device. To reassign the virtual disk, use the **vDisk Properties Assign vDisk** dialog on the console.

Nutanix Acropolis requirements

The following are required when using Citrix Provisioning with Nutanix Acropolis:

- An installed Nutanix Acropolis hypervisor plug-in for Citrix Provisioning. Download this plug-in from the Nutanix support site. See the Nutanix documentation portal for installation information.
- A Citrix Virtual Apps and Desktops host connection to AHV.
- Nutanix Acropolis platform version 5.1.1 or greater.

> **Tip:**
>
> Unique to AHV provisioning is the requirement to choose a container.

Important considerations when using Nutanix Acropolis hypervisors

When using Nutanix, consider the following:

- Do not delete the NIC of a provisioned VM and then readd them.
- BDM partition is not supported.

- Only the Citrix Virtual Apps and Desktops Setup Wizard is supported, not the Streamed VM Wizard.
- Acropolis hypervisors use snapshots and not templates for VMs.
- Ideally, a snapshot does not have an attached hard disk because the Nutanix Acropolis hypervisor does not remove the hard disk during provisioning.
- When you deploy machines that boot from BDM ISOs, the ISO is mounted in the snapshot. The provisioned VMs are set to use PXE boot. Even though PXE was selected in the Setup Wizard, the deployed VMs honor the template snapshot. These VMs boot to the BDM ISO without extra steps as long as the template snapshot contains the BDM ISO and the default boot order.
- For PXE booting, change the boot device for a UEFI VM by using only the UEFI firmware menu.
- You can add Nutanix hosts only by using the Citrix Virtual Desktops Setup Wizard from a Citrix Virtual Apps and Desktops Setup Wizard hosting connection.

> **Note:**
>
> For information about Nutanix Acropolis hypervisors, see the Nutanix documentation portal.

Implementing UEFI guest VMs for Nutanix AHV hosts

Citrix Provisioning allows you to implement a UEFI guest VM for Nutanix AHV hosts. The following prerequisites exist:

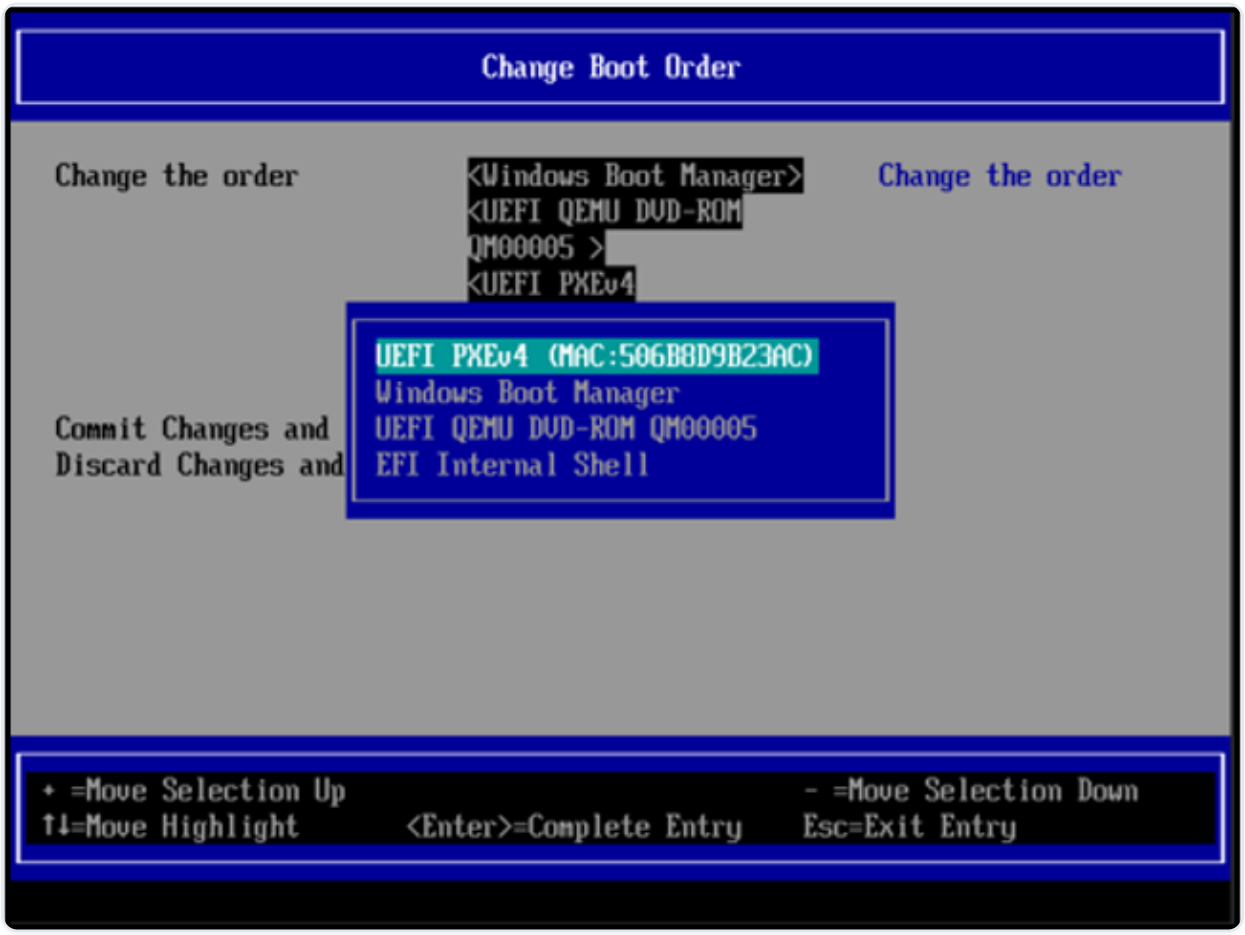
- The Citrix Virtual Apps and Desktops DDC are installed, along with the Nutanix plug-in.
- The Nutanix plug-in is installed in the provisioning server and provisioning console.

> **Note:**
>
> The VM is set to UEFI before installing the OS.

To implement a UEFI guest VM for Nutanix AHV:

1. Create a master VM.
2. SSH into Nutanix Acropolis and run the following command: `acli vm.update <VM_NAME> uefi_boot=True`.

3. Mount the Windows and virtual ISOs and install the OS.
4. Install all Windows updates on the OS.
5. Join the OS to Active Directory.
6. Install Citrix Provisioning on the target device.
7. Run the Citrix Provisioning Imaging Wizard to create the target device record, virtual disk, and other elements. Select **No** to shut down the target device, rather than rebooting it at the conclusion.
8. Set up the boot device for a UEFI VM. You can change the boot device for a UEFI VM by using only the UEFI firmware menu.



For more information, see Setting up Boot Device.

9. Start the VM and log into Windows to start the second stage of Imaging Wizard, *imaging*.
10. Create a VM. As in the master VM, repeat steps 2 and 7.
11. In the provisioning console, create a VM record for the snapshot VM using the VM's MAC address. Assign the virtual disk created in step 7 to this device record.
12. Boot the VM. Install the VDA, and restart if prompted. Shutdown when the installation finishes.
13. Create a snapshot of this VM.

14. In the provisioning console, set the virtual disk to **standard image mode**. If the cache mode is **Cache on device hard disk** or **Cache in device RAM with overflow to hard disk**, the wizard prompts you to create a cache disk.
15. Use the Citrix Virtual Apps and Desktops setup Wizard to provision UEFI provisioning target devices using the created virtual disk.

SCVMM requirements

You cannot provision vGPU-enabled VMs on Hyper-V.

Limitation:

HyperV Gen1 VMs provisioned using Citrix Virtual Apps and Desktops Setup Wizard always have the operating system set to unknown instead of the operating system of the template.

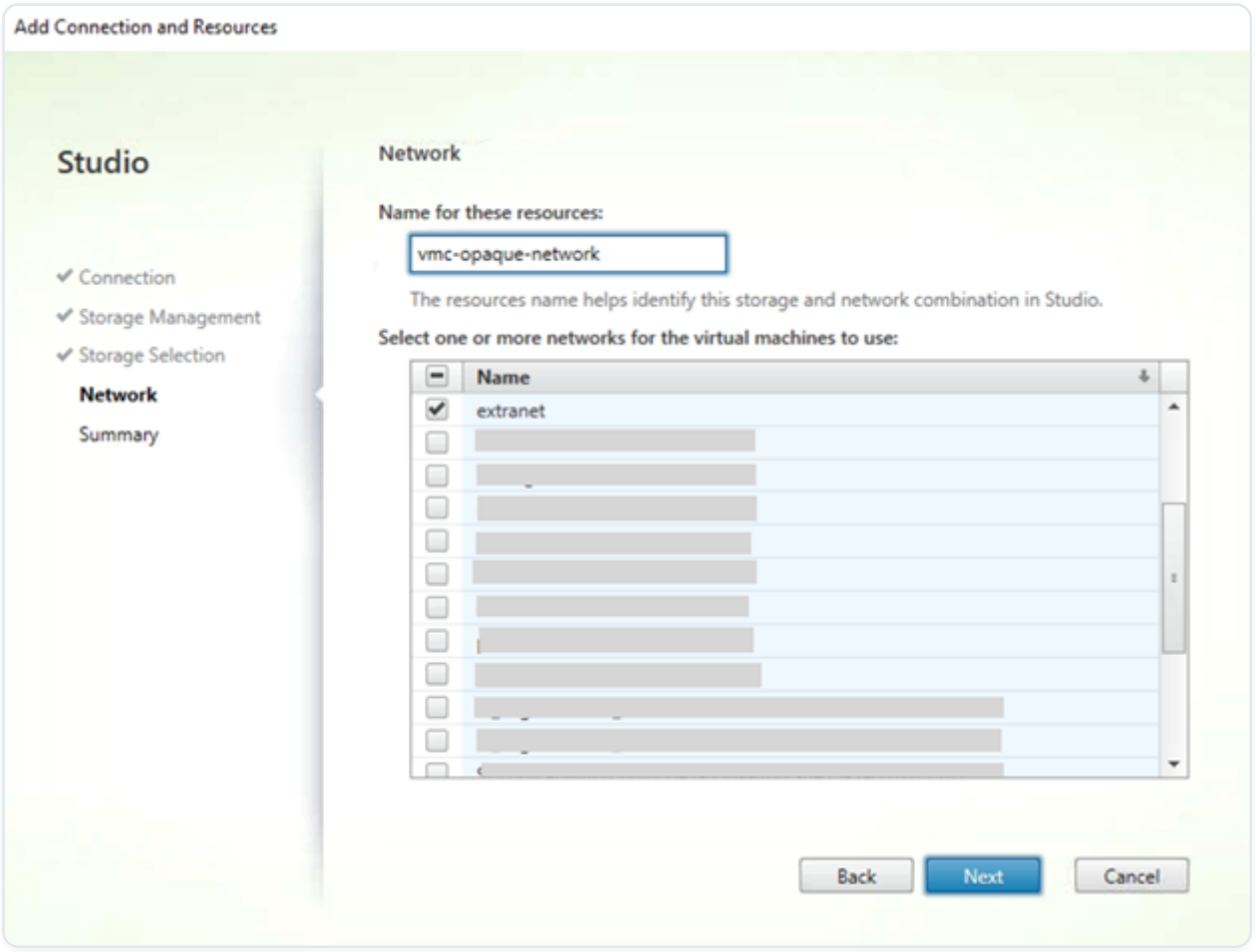
Provision VDAs on an opaque Network

To provision a VDA on an opaque network, use the Citrix Virtual Apps and Desktops Setup Wizard.

Create the hosting unit and associate the opaque network to it using Citrix Studio. See Connections and resources for more information.

Use Citrix Studio to select an opaque network

In Citrix Studio, access the **Add Connection and Resources** page. In the **Network** section, select the resource representing the opaque network, then click **Next**:



Tip:

After creating a hosting unit with the opaque network, use it in the Citrix Virtual Apps and Desktops Wizard in the provisioning console.

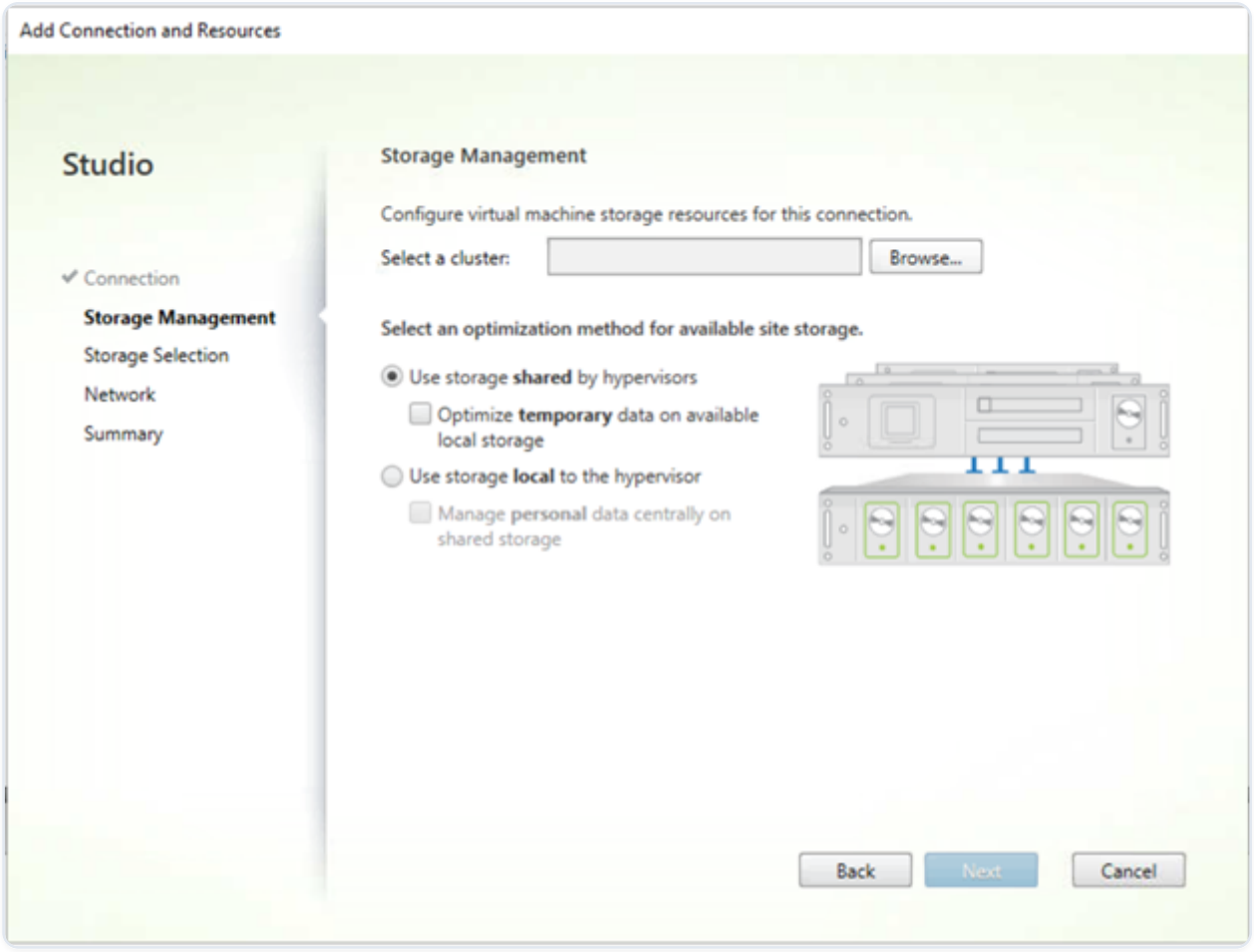
Provision VDAs to a specific resource pool

Citrix Provisioning supports provisioning VDAs at a specific resource pool in an on-premises ESX hypervisor. You can provision this VDA using the Citrix Virtual Apps and Desktops Setup Wizard in the Citrix Provisioning console.

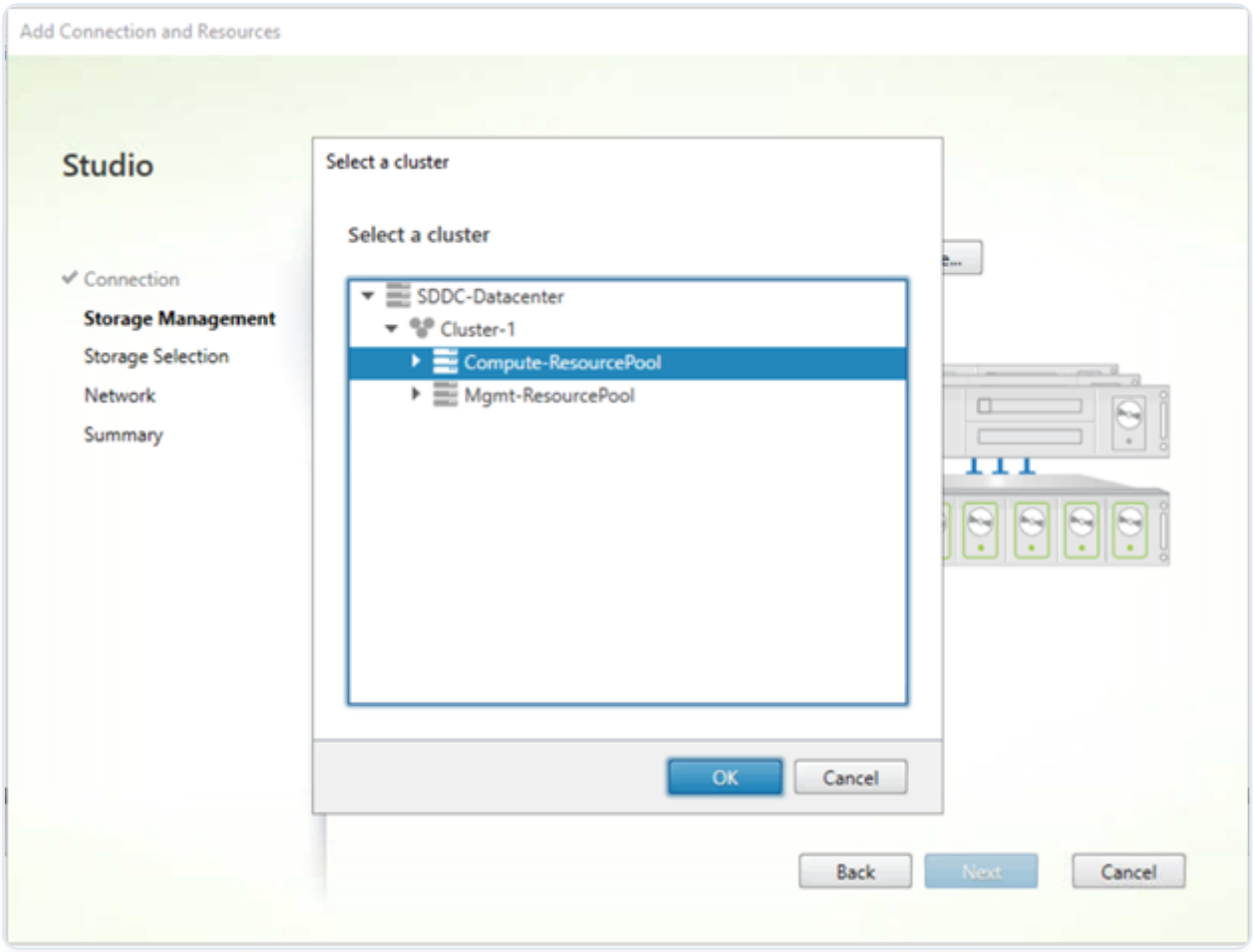
Note:

Create a hosting unit with the resource pool using Citrix Studio before using the Setup Wizard in the provisioning console.

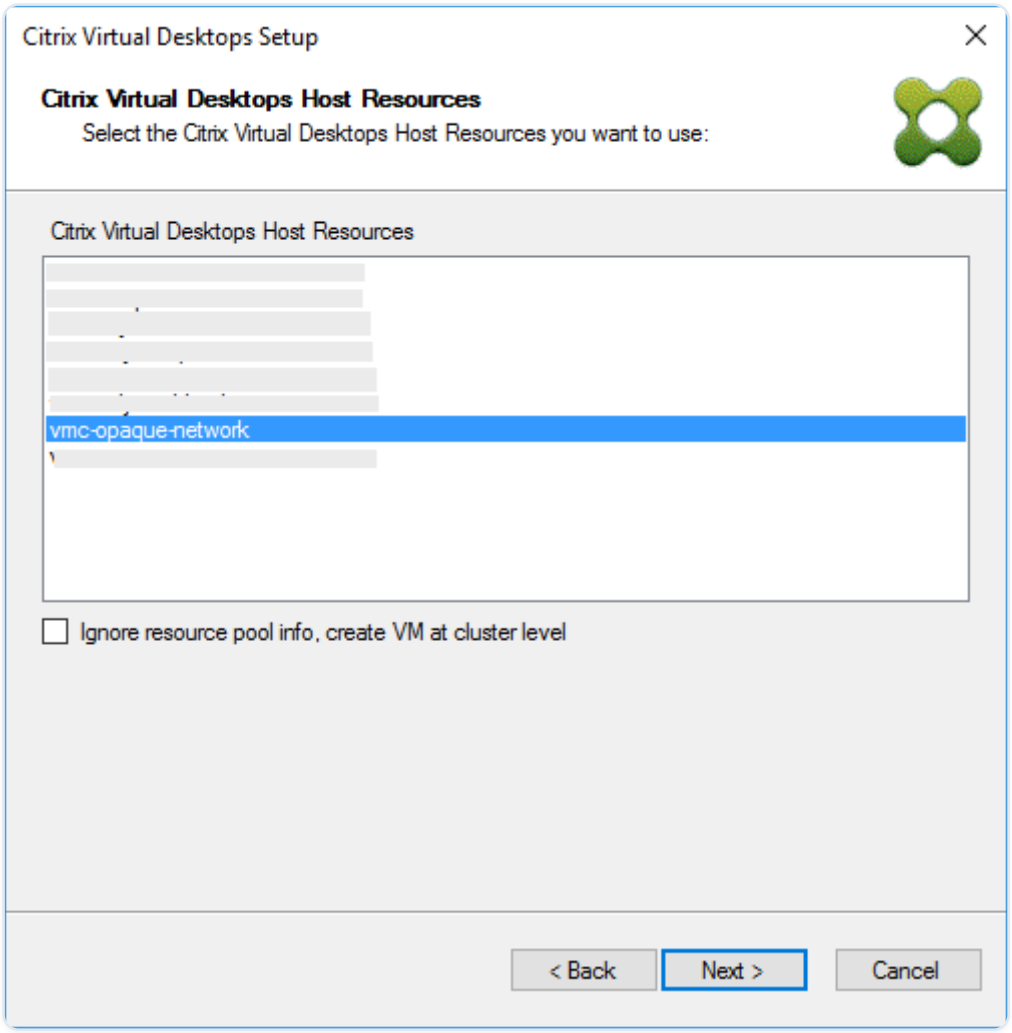
- The provisioned target device installer registers the WMI and performance counter providers. No additional installation options require configuration on the provisioned target device.
- The current `CVhdMp` performance counter provider only supports VHDX for target devices using **Cache in device RAM with overflow on hard drive**. Configure the resource pool. In Citrix Studio, launch the **Add Connection and Resources Wizard**. From the **Add Connection and Resources** page, select **Storage Management**. In the **Select a cluster** field, click **Browse**:



Select the appropriate cluster, and click **Next**. Select the `Compute-ResourcePool` or any of the child resource pool options under `Compute-ResourcePool`.



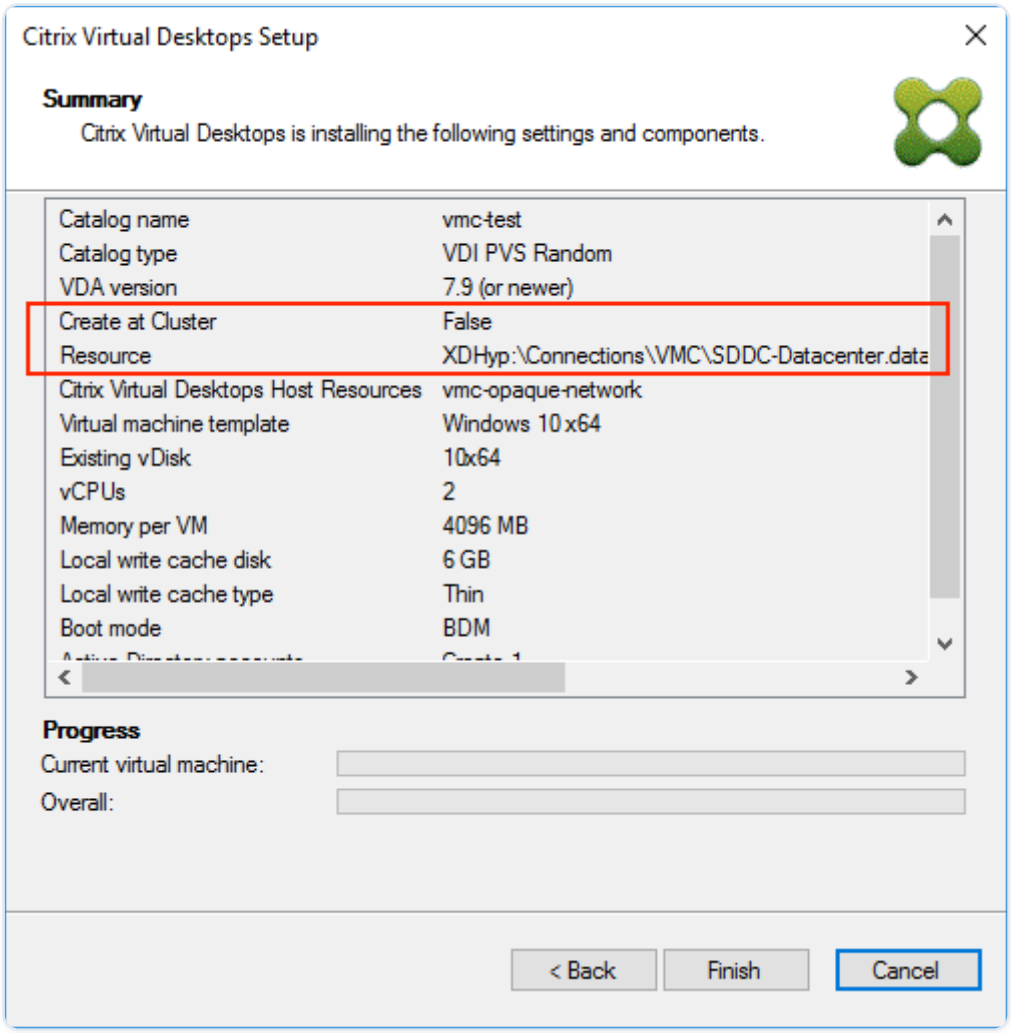
Use the Citrix Virtual Apps and Desktops Setup Wizard in the provisioning console to select the hosting unit with the resource pool. Click **Next**:



Tip:

To provision at the root cluster level, select the **Ignore resource pool info, create VM at cluster level** checkbox.

The cluster and the resource pool info appear in the Summary page of the Citrix Virtual Apps and Setup Wizard:



Using PowerShell to provision VDAs at the resource pool level

Citrix Provisioning 1912 includes a new switch parameter, `UseResourcePool`, added to `StartPvsProvisionXdMachines` in the `Citrix.ProvisioningServices` PowerShell cmdlet.

To provision machines at the resource pool level, use the `Start-ProvisionXdMachines` with the `-UseResourcePool` switch parameter.

For example:

```
Start-PvsProvisionXdMachines -DdcAddress <ddcAddress> -BootType <bootType>
-CatalogName <catalogName> -CatalogDescription <catalogDescription>
-SessionSupport <sessionSupport> -AllocationType <allocationType>
-PersistUserChanges <persistUserChanges> -Scope <scope> -VdaLevel
<vdaLevel> -XenDesktopHostResource <hostname> -HostResourcePassword
<hostPassword> -TemplateName <templateName> -NetworkPath <networkPath>
-StoreId <storeId> -SiteId <siteId> -DiskLocatorId <diskLocatorId> -Domain
<domain> -OrganizationalUnit <organizationalUnit> -NamingScheme
<namingScheme> -VmCount <vmCount> -DeviceMemory <deviceMemory> -DeviceCpu
```

```
<deviceCPU> -DeviceWriteCacheSize <deviceWriteCacheSize> -NameSuffixType
<nameSuffixType> -VmPvdSize <vmPvdSize> -VmPvdDrive <vmPvdDrive>
-UseResourcePool
```

Note:

If the parameter `-UseResourcePool` is not included, the VDA is provisioned at the root cluster level.

Provisioning vGPU-enabled Citrix Virtual Apps™ and Desktop machines

XenServer (formerly Citrix Hypervisor)/ESX hypervisor supports NVIDIA virtual GPU (vGPU) solutions that consist of NVIDIA data center GPUs and vGPU software licensing components. The underlying data center GPUs in the XenServer host is unknown to Citrix Provisioning. Citrix Provisioning only uses the vGPU software settings in the template and propagates it to the VMs provisioned by the Citrix Virtual Apps and Desktops Setup Wizard.

Requirements

- An NVIDIA vGPU certified server capable of hosting XenServer® and NVIDIA vGPU software.
- Supported hypervisors: Nutanix AHV, Citrix XenServer 6.2 or newer, or vSphere 6.0 or newer.
- NVIDIA vGPU software: NVIDIA vApps, vPC or RTX Virtual Workstation.
- NVIDIA drivers: NVIDIA Graphics Driver or NVIDIA RTX Enterprise Driver.
- The Citrix Provisioning release that corresponds to the Citrix Virtual Apps and Desktops™ release you are using. The Citrix Virtual Apps and Desktops Setup Wizard only supports the corresponding Citrix Virtual Apps and Desktops controller.
- To provision machines using the Citrix Virtual Apps and Desktops Setup Wizard, you must use Citrix Provisioning™ 1912 LTSR or later.

Note:

Citrix Virtual Apps and Desktops supports power management for virtual machine (VM) catalogs, but not for physical machine catalogs.

Provisioning procedures

Prepare the master VM

1. Prepare the master VM with vGPU enabled.
2. Install the NVIDIA drivers.
3. Join the machine operating system to Active Directory.
4. Install the Citrix Provisioning target device software.
5. Using the Citrix Provisioning Imaging Wizard, create a master virtual disk image. If you plan to use the Citrix Virtual Apps and Desktops Setup Wizard to provision machines, select the Target Device Optimizer option.
6. Create a template from the master to use during provisioning, using the CVAD Setup Wizard.

Prepare the template VM

Use the information in this section to set up a template VM for provisioned targets. When preparing the template VM, consider:

- the template uses an attached write cache. This cache is small, approximately 8–16 MB, and can be used for environments requiring a workaround for the SAN policy method.
- the write cache can also be used in environments applying the UseTemplateCache method.
- the attached disk ensures that the provisioned target device recognizes the storage controller.
- booting a VM is a verification process ensuring that the VM used as a template functions with the virtual disk. If the template VM does not boot, the failure is recognized quickly without waiting to provision more VMs.

To prepare the template VM:

1. Create a template VM with the same properties as the master VM. Assign a hard drive to the template VM to use for write cache.
2. Create a device record in the Citrix Provisioning database with the MAC address of the template VM.
3. Assign the virtual disk to the template VM, and then set the device to boot from virtual disk.
4. PXE boot the VM.
5. Format the write-cache disk.

Install the Citrix Virtual Apps and Desktops Virtual Delivery Agent

1. Using the Citrix Provisioning console, set the virtual disk image mode to **Private Image**.
2. Install the Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA) and point the VDA to the Citrix Virtual Apps and Desktops Server during the installation. **Note:** Alternatively, you can install both the VDA and the target device software before creating the virtual disk image. Both install methods require the new template VM to have a formatted write-cache hard drive.
3. Reboot the VM, and then shut the VM down.
4. Convert the VM to a template.

Create Citrix Virtual Apps and Desktops VMs

1. Using the Citrix Provisioning console, set the virtual disk image mode to **Standard Image**.
2. Choose the preferred write cache method.
3. Select from the following provisioning methods:
    - Deploying virtual desktops to VMs using the Citrix Virtual Apps and Desktops Setup Wizard
    - Using the Streamed VM Setup Wizard

Create Citrix Virtual Apps and Desktops machine catalogs

When choosing between creating physical or virtual/blade server machine catalogs, it is important to consider the different advantages and requirements. For example, VM machine catalogs allow for power Citrix Virtual Apps and Desktops management while physical machine catalogs do not.

Physical machine catalogs

Device names must exist in Citrix Provisioning device collection and in Active Directory.

> **Tip:**
>
> The Citrix Virtual Apps and Desktops host record is not required and the VM record names are not verified.

1. Start the Citrix Virtual Apps and Desktops Machine Catalog Setup Wizard, then select **Windows Desktop OS** on the **Operating System** page.
2. On the **Machine Management** page, for **This Machine Catalog uses** select **Machines that are not power managed**, for example, physical machines.

3. For **Deploy machines using:** select **Citrix Provisioning**. Power management is not provided by Citrix Virtual Apps and Desktops.
4. For **User Experience** select **Users connect** to a random desktop each time they log on.
5. Enter the provisioning server's IP address for the device collection.
6. Identify the domain where all device Active Directory records are stored and the VDA version level, then click **Connect**.
7. In the structure that appears, select the **Citrix Provisioning device** collection where all the vGPU devices are located, and then click **Next**. Device records are stored in an exclusive device collection.
8. Enter a machine catalog name and description, and then click **Finish**.

Create a Delivery Group and associate it with the machine catalog

For details on creating a Delivery Group, see the Citrix Virtual Apps and Desktops documentation.

Citrix Provisioning and Citrix Virtual Apps and Desktops cloud considerations

Within a cloud, you create a machine catalog and deploy it to those machines using Citrix Provisioning by pointing the catalog to a provisioning collection. If you use Citrix Provisioning with a cloud, all the machines within the provisioning collection must be associated with Active Directory accounts.

For more information, see Citrix Provisioning managed by Citrix Cloud.

Citrix Provisioning™ Accelerator

Citrix Provisioning Accelerator optimizes the capability of Citrix Provisioning services and is available only on XenServer.

Some of the benefits of using Citrix Provisioning Accelerator are:

- Less administration time
- Greater employee productivity
- Decreased security vulnerability window
- Save money on storage and networking
- More scalability on existing infrastructure
- Faster deployments of more users and desktops

- More GTM and increased business agility

Note:

- PVS-Accelerator is available for XenServer Premium Edition customers. To use the PVS-Accelerator feature, upgrade the Citrix License Server to version 11.14 or later.
- To use PVS-Accelerator with UEFI-enabled VMs, use Citrix Provisioning 1906 or later.
- To enable Citrix Provisioning Accelerator for targets using IPv6 streaming use XenServer8.

How does PVS-Accelerator work

Citrix Provisioning Accelerator enables a provisioning proxy to reside in Dom0 (the XenServer Control Domain) on a XenServer host. This is the location where streaming of a provisioning virtual disk is cached at the proxy before being forwarded to the VM. Using the cache, subsequent VM booting (or any I/O requests) on the same host are streamed from the proxy rather than streaming from the server over the network. Using this model, more local resources on the XenServer host are consumed, but streaming from the server over the network saves resources, effectively improving performance.

Considerations

Consider the following when using the PVS-Accelerator feature:

- Citrix Provisioning target devices are aware of their proxy status. No additional configuration is required once the capability is installed.
- Do not disable Citrix Provisioning Accelerator on a VM using the XenCenter. If you do, provisioning fails to recognize the configuration change and continues to believe that the accelerator feature is enabled on that VM. If you want to disable this feature for a single device, see:
  - Enable or disable Citrix Provisioning Accelerator for individual devices
  - Disable Citrix Provisioning Accelerator for all devices on a host

Limitations

- In environments where multiple Citrix Provisioning servers are deployed with the same VHD, but have different file system timestamps, data might be cached multiple times. Due to this limitation, we recommend using VHDX format, rather than VHD for virtual disks.
- After reinstalling XenServer, the accelerator cache remains configured in the Citrix Provisioning database. This process causes an error in the VM setup wizard because Citrix Provisioning assumes that the cache still exists. To resolve this issue, delete and then add the XenServer host using the provisioning console. This procedure enables Citrix Provisioning to clear the stored cache configuration. After the stored cache configuration has been cleared, the administrator can create one in XenCenter.

Enable Citrix Provisioning Accelerator

Complete the following configuration settings in XenServer and in Citrix Provisioning to enable the Citrix Provisioning Accelerator feature:

1. Configure Citrix Provisioning Accelerator in XenServer by using XenCenter or the xe CLI. This configuration includes adding a Citrix Provisioning site and specifying the location for Citrix Provisioning cache storage.

   - For information about configuring the PVS-Accelerator using the xe CLI, see Configure PVS-Accelerator in XenServer by using the CLI.
   - For more information about configuring the PVS-Accelerator using XenCenter, see Enabling PVS-Accelerator.

   For information on specifying the location for Citrix Provisioning cache storage, see:

   - Configure cache storage on a storage repository
   - Configuring cache storage in the control domain memory

2. Complete the cache configuration for the Citrix Provisioning Site using the Citrix Virtual Desktops™ Setup Wizard or Streamed VM Setup Wizard. See Configure cache in Citrix Provisioning

Configure cache in Citrix Provisioning

Before doing this, create a Citrix Provisioning Site object. For information, see Enable PVS-Accelerator.

Use the **Citrix Virtual Desktops Setup Wizard** or **Streaming VM Wizard** (depending on your deployment type) to access the Proxy capability. Although both wizards are similar and share many of the same screens, the following differences exist:

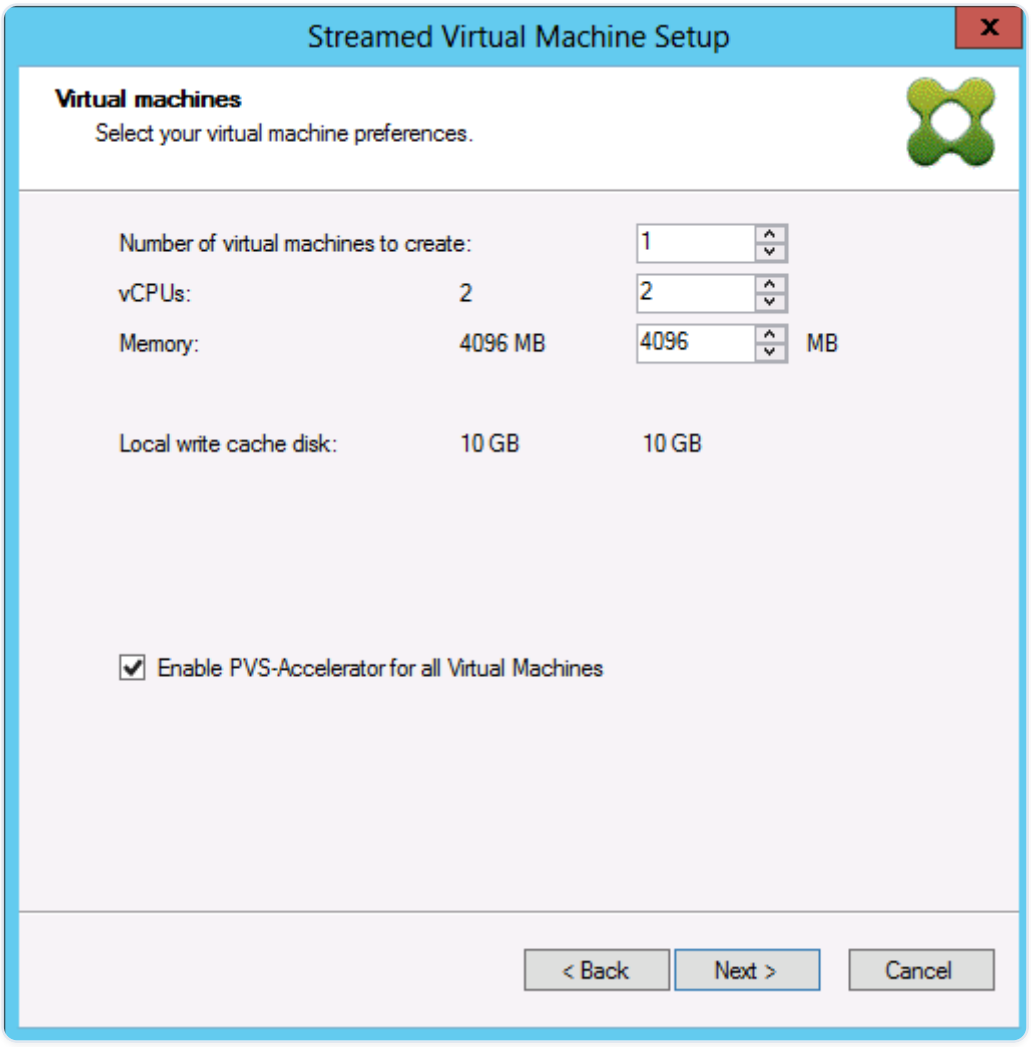
- The Citrix Virtual Desktops Setup Wizard is used to configure VMs running on the XenServer hypervisor that is controlled using Citrix Virtual Desktops.
- The Streaming VM Wizard is used to create VMs on a host. It does not involve Citrix Virtual Desktops.

To configure Citrix Provisioning Accelerator using the provisioning console:

1. Use the Configuration Wizard to assign IPv4 and IPv6 streaming addresses to Citrix Provisioning Servers. See Select network addresses for the stream service.

   > **Note:**
   >
   > To enable Citrix Provisioning Accelerator for targets using IPv6 streaming, use XenServer8.

2. Navigate to the site where this Citrix Provisioning server is a member.
3. Select the site, then right-click to expose a contextual menu.
4. Select the appropriate Wizard based on how you intend to use the accelerator feature.
5. Select the option **Enable PVS-Accelerator for all Virtual Machines** to enable the PVS-Accelerator feature.



6. If you are enabling virtual disk caching for the first time, the **XenServer** screen appears on the **Streamed Virtual Machine Setup** wizard. It displays the list of all Citrix Provisioning sites configured on XenServer that have not yet been associated with a Citrix Provisioning site. Using the list, select a Citrix Provisioning site to apply PVS-Accelerator. This screen is not displayed when you run the wizard for the same Citrix Provisioning site using the same XenServer.
7. Click **Next** to complete the caching configuration.
8. Click **Finish** to provision Streamed VMs and associate the selected Citrix Provisioning site with the PVS Accelerator in XenServer.
9. When this step is complete, the **View PVS Servers** button in the **PVS-Accelerator configuration** window is enabled in XenCenter. Click **View PVS Servers** to display the IP addresses of all PVS Servers associated with the Citrix Provisioning site. You must see all IPv4 and IPv6 addresses.

Troubleshoot

When a proxy cache configuration is tied to a provisioning server and you reinstall XenServer on the host that had the accelerator feature enabled, Citrix Provisioning and XenServer become out of sync. This occurs because the reinstallation of XenServer wipes the previously configured proxy cache configuration. Reconfiguration of Citrix Provisioning server also causes the previously configured Citrix Provisioning site object to become out of sync.

In this scenario, Citrix Provisioning assumes that the proxy cache configuration still exists, and when the Streamed VM Setup Wizard is used, it fails. This process indicates that the provided UUID (associated with the proxy configuration) is invalid.

To resolve the issue, delete all previously configured VMs associated with this cache configuration, including the host. Reconfigure Citrix Provisioning and set up the cache again.

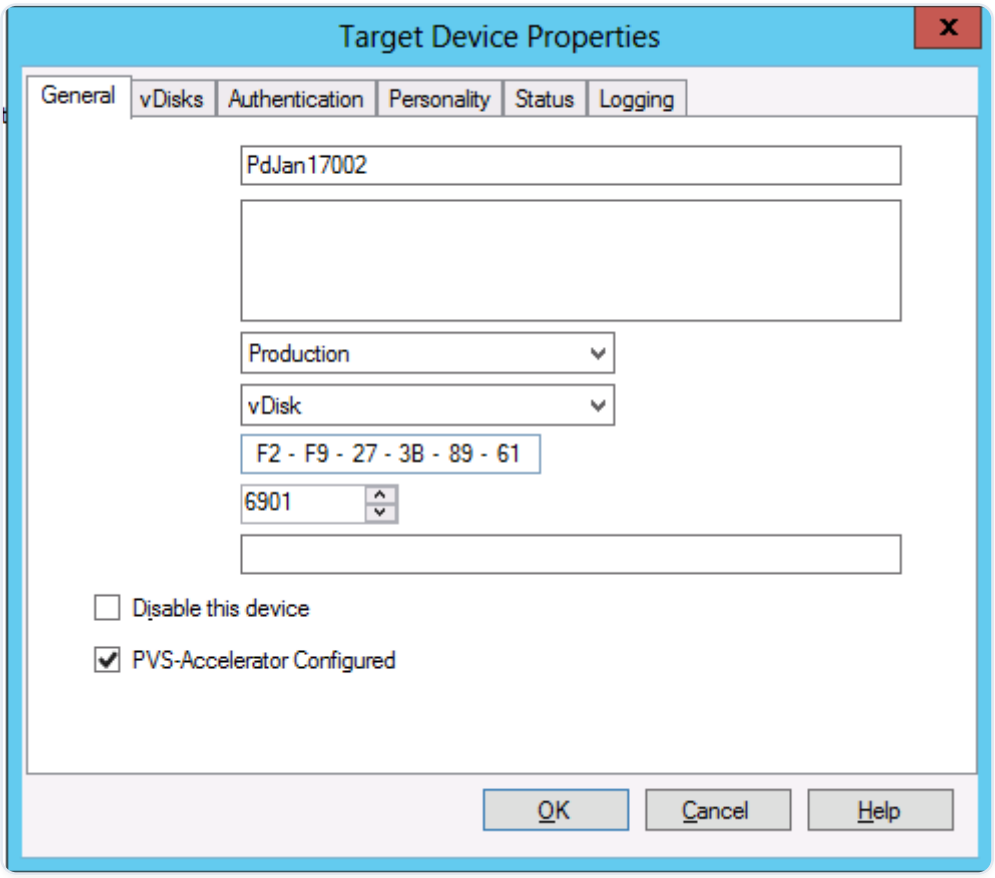
Enable or disable Citrix Provisioning Accelerator for individual devices

Use the **Target Device Properties** screen to enable or disable the feature for an individual device.

> **Note:**
>
> Do not disable the Citrix Provisioning Accelerator on a VM using the XenCenter. If you do, provisioning fails to recognize the configuration change and continues to believe that the accelerator feature is enabled on that VM.

To enable or disable this feature for an individual device:

1. Go the **Target Device Properties** screen.
2. In the **General** tab, select (or deselect) **PVS-Accelerator Configured**.
3. Click **OK** to apply the change.



Disable Citrix Provisioning Accelerator for all devices on a host

If you enable PVS-Accelerator for a host, you can disable it using the **Virtual Host Connection Properties** screen for all devices on the specified host.

> **Important:**
>
> You cannot use the **Virtual Host Connection Properties** screen to enable PVS-Accelerator on the specified host. Enable the feature using one of the Wizards (Citrix Virtual Apps and Desktops™ Setup Wizard or Streamed VM Wizard) while creating devices.

To disable this feature for all devices on the specified host:

1. Access the **Virtual Host Connection Properties** screen.
2. In the **General** tab, select (or deselect)**PVS-Accelerator Enabled**.
3. Select **Yes** when you are prompted to confirm the action.
4. After verifying the action, click **OK** to apply the change.

Unified Extensible Firmware Interface (UEFI) pre-boot environments

Citrix Virtual Apps and Desktops™ supports Unified Extensible Firmware Interface (UEFI) hardware technology on all virtualization environments. Citrix Provisioning supports streaming of only UEFI based targets.

UEFI is a complete replacement for BIOS and requires a new bootstrap. One bootstrap file for 64-bit systems is available.

When configuring UEFI, install the OS disk in a VM configured to use UEFI boot. Once you install the OS disk, Windows automatically configures the boot disk to use the GUID partition table (GPT) file system.

Limitation

UEFI target boot menu supports a maximum of nine entries.

Secure boot in UEFI

Citrix Provisioning™ supports Secure Boot in UEFI on these platforms:

- Physical machines with UEFI firmware and the Secure Boot option.
- Hyper-V 2016 and later VMs that use the Microsoft UEFI Certificate Authority template in the **Secure Boot** setting. Hyper-V 2012 R2 is not supported.
- ESX version 6.7 or later, and 7.0 update 3.
- Nutanix AHV 6.5 LTS or later.
- XenServer 8.0
- Guest UEFI boot and secure boot are supported on Citrix 8.1 Hypervisors. See the XenServer documentation for more information.

Network topology

When booting targets over the network, the Citrix Provisioning PXE server provides the simplest setup because the PXE protocol supports multiple architectures. The Citrix Provisioning PXE Server recognizes the architecture flag embedded in DHCP, then discovers and returns the appropriate bootstrap file name. If you want to support network boot of both legacy BIOS and UEFI targets on the same broadcast network, then you must enable the Citrix Provisioning PXE Service and remove any DHCP options related to specifying the bootfile from the regular DHCP setup.

If DHCP option 67 is chosen, there are two topology options:

- On a single segment, use DHCP reservations to specify the bootstrap file name (option 67) for every target device. This process is feasible for smaller environments but quickly scales out of hand for enterprise environments. Use this option if you want to support both legacy BIOS and UEFI on the same segment.
- Divide the environment into multiple segments, isolating the legacy devices from the UEFI devices. For each segment, configure a DHCP scope with the appropriate option 67 set.

Configuring bootstraps

The UEFI bootstrap does not have embedded settings. DHCP options are therefore used to configure the UEFI bootstrap.

> **Remember:**
>
> Citrix Provisioning supports only UEFI network booting.

DHCP option 11 – RLP server

Option 11 allows you to specify multiple IPv4 addresses. Use this option to specify the addresses of the streaming NICs on the provisioning server. You can specify more than four addresses. The UEFI bootstrap reads all addresses, picks a random address from the list, and connects to that address. If the connection fails, then UEFI bootstrap tries the remaining addresses in a round-robin manner.

> **Note:**
>
> Option 17 takes precedence over option 11.

DHCP option 17 – root path

The root path option can be used to provide a single DNS FQDN, IPv4, or IPv6 address to connect to the targets. When using IPv6 streaming, this option is mandatory. Multiple login servers can be implemented by creating a DNS alias that translates to the list of up to 32 login servers.

```
pvs:[Address]: 17:6910



pvs – Required identifier



Address – IPv4, IPv6 or DNS FQDN referencing the streaming NIC on one or
more PVS servers



17 – Protocol identifier for UDP (can be omitted if the default login port
is used)



port – Logon port (not required if the default port of 6910 is used)
```

Examples:

```
pvs:[server.corp.com]:17:6910



pvs:[192.168.1.1]:17:6910



pvs:[fc02::2bfa:5e30:3631:fef4]:17:6910
```

Citrix Provisioning™ managed by Citrix Cloud

Citrix Provisioning supports Citrix Cloud™ integration. It enables provisioned VDAs to be used in Citrix DaaS.

Important considerations:

- Configure the Citrix Provisioning console (or use associated PowerShell commands) to use the Citrix Cloud license.
- Check your Citrix Licensing server and ensure you are using either a Citrix Provisioning Enterprise or Platinum license version.
- Once you choose to join your farm to Citrix Cloud, the association is permanent and cannot be reversed. You also cannot change the customer to which the farm is linked.
- To install the Remote PowerShell SDK for use with Citrix Cloud Government, run the command `CitrixPoshSdk.exe EnvironmentName=USGovernment`. For more information, see SDKs.

What's required

The following elements are required when using Citrix Provisioning with Citrix Cloud:

- **Citrix Virtual Apps and Desktops™ Delivery Controller in Citrix Cloud:** Citrix Provisioning supports working with both customer managed and Citrix Cloud Delivery Controllers natively from the same Citrix Provisioning Console.
- **Citrix Cloud Connector™ located on-premises:** The Cloud Connector provides services for the Citrix Cloud Delivery Controllers to configure the resource location where Citrix Provisioning runs.
- **Provisioning Server located in the resource location where Citrix Provisioning targets must run:** Citrix Provisioning server must be 1912 LTSR or later for on-premises, 2203 LTSR or later for Citrix Provisioning on Azure, and 2206 or later for Citrix Provisioning on GCP.
- **The Citrix Licensing Server available in the customer managed location:** This can be either on-premises or in a cloud subscription managed by the customer.

Note:

- Do not install on-premises Citrix Virtual Apps™ and Desktops PowerShell SDK or upgrade the Citrix Virtual Apps and Desktops Remote PowerShell SDK on the system running the Citrix Provisioning console. This is because the console depends on the version installed with that package.
- Do not install Citrix Provisioning on the Delivery Controller™ or the machine on which Citrix Studio is installed.
- If you want to run scripts using the Citrix Virtual Apps and Desktops PowerShell SDK on the same system as the console, then configure the system to communicate with either

> Citrix Cloud or customer managed Delivery Controller as required. The default is to communicate with Citrix Cloud.

Dependencies

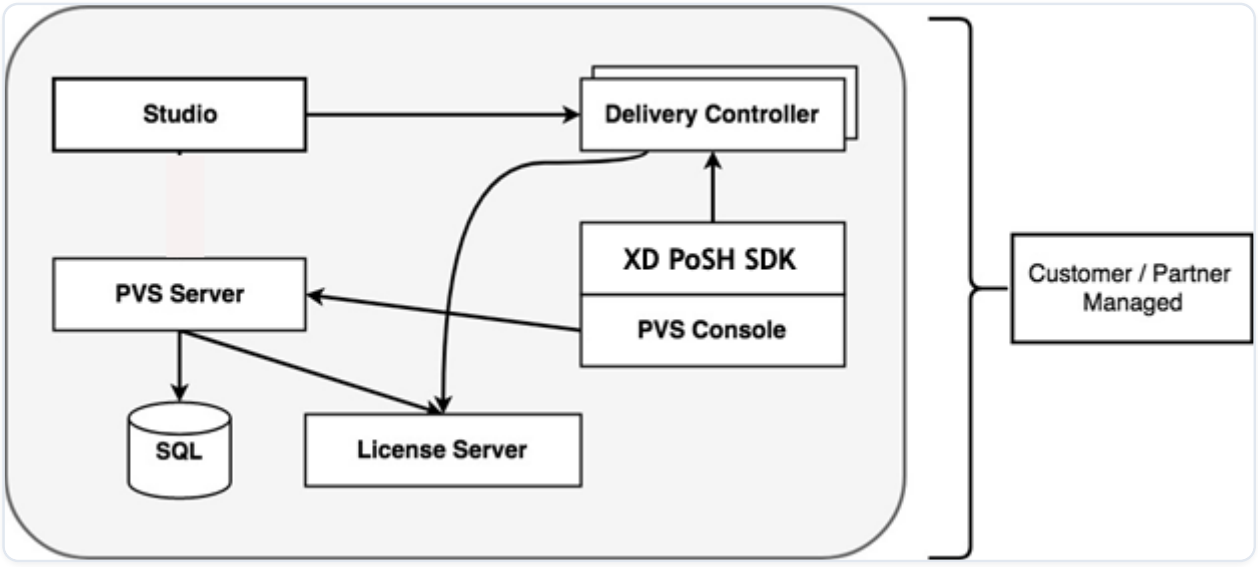
The following dependencies exist when using Citrix Provisioning and Citrix Cloud:

- Citrix Studio
- Citrix Cloud Connector

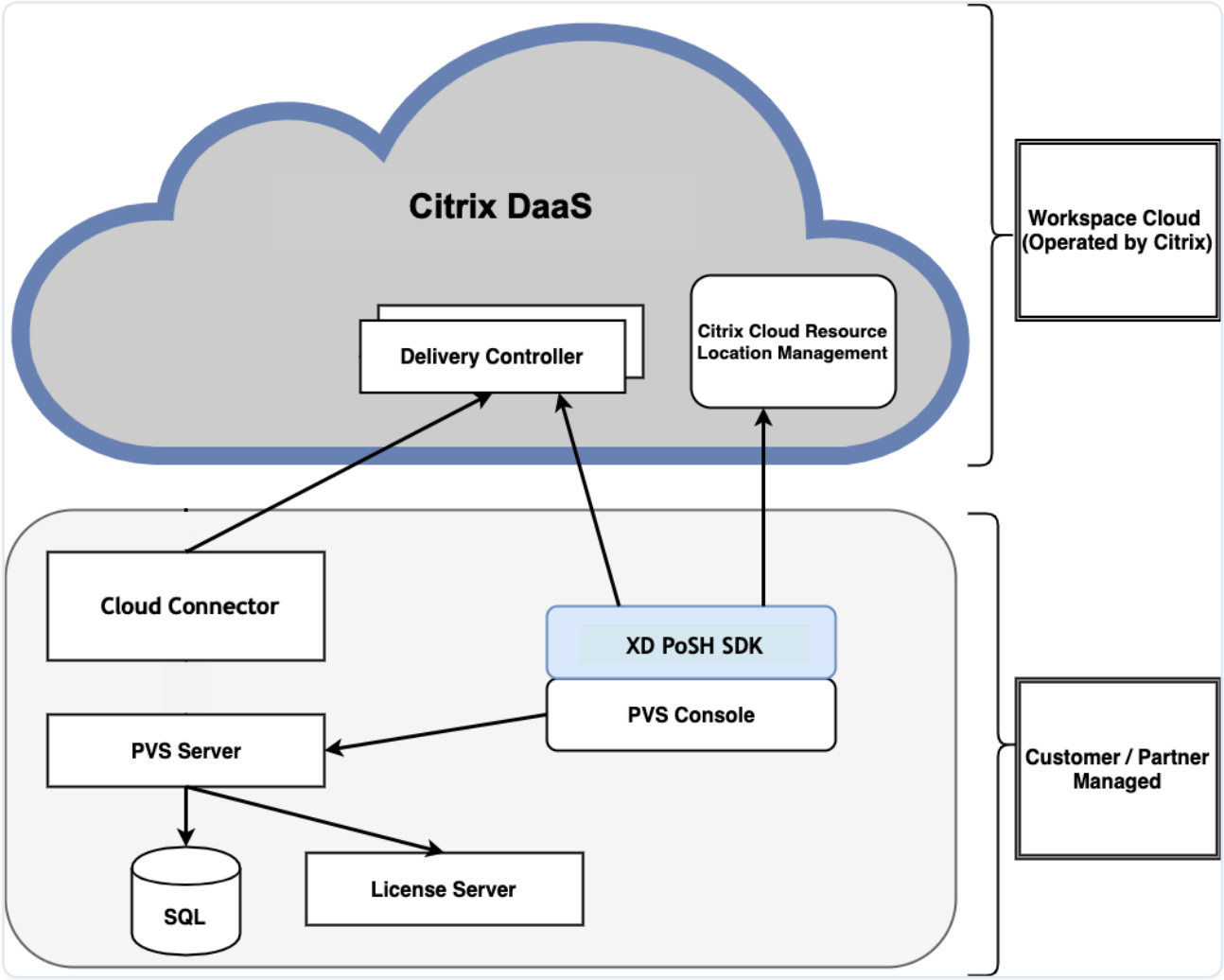
On-premises versus Citrix Cloud deployments

Citrix Provisioning supports working with both customer managed and Citrix Cloud Delivery Controllers natively from the same Citrix Provisioning Console.

Traditional Citrix Virtual Apps and Desktops deployments using Citrix Provisioning require the management of two distinct elements: both the Citrix Virtual Apps and Desktops deployment and the Citrix Provisioning deployment. Such environments resemble the following image, without the added complexity of illustrating VDA components:



With an on-premises Citrix Provisioning deployment, the Citrix Virtual Apps and Desktops have been extended:



Extending the Citrix Virtual Apps and Desktops deployment eliminates the need to operate and manage the deployment while still providing the benefits of a managed Citrix Provisioning deployment.

Citrix Provisioning adds provisioning managed VDAs to a machine catalog in the Citrix Virtual Apps and Desktops Delivery Controller located in Citrix Cloud. This process adds new devices using the Citrix Virtual Apps and Desktops Setup Wizard in the provisioning console.

Citrix Virtual Apps and Desktops Setup wizard in the Citrix Provisioning console

The Citrix Virtual Apps and Desktops Setup Wizard enables you to create Citrix Provisioning devices and collections, and then create machine catalogs containing these elements.

Connecting your Citrix Provisioning deployment to the Citrix Virtual Apps and Desktops in Citrix Cloud

Citrix Provisioning supports working with both customer managed and Citrix Cloud Delivery Controllers natively from the same Citrix Provisioning Console.

To connect an existing Citrix Provisioning deployment to Citrix Cloud, upgrade Citrix Provisioning. The Citrix Provisioning server must be 1912 LTSR or later for on-premises, 2203 LTSR or later for Citrix Provisioning on Azure, and 2206 or later for Citrix Provisioning on GCP. The recommended version is the latest CU of one of the LTSRs: 1912 or 2203, or latest CR. See the download page.

Upgrade Citrix Provisioning

To use Citrix Cloud with Citrix Provisioning, you must use a version that integrates with the Citrix Virtual Apps and Desktops. The Citrix Provisioning server must be 1912 LTSR or later for on-premises, 2203 LTSR or later for Citrix Provisioning on Azure, and 2206 or later for Citrix Provisioning on GCP. The recommended version is the latest CU of one of the LTSRs: 1912 or 2203, or latest CR.

Firewall considerations

Firewall configurations typically require zero or minimal updates. Consider the following:

- On the Provisioning Console, outward bound SDK traffic uses HTTPS (port 443).

For more information about cloud connector connectivity requirements, see Cloud Connector common service connectivity requirements and Firewall Configuration.

Administer VDAs

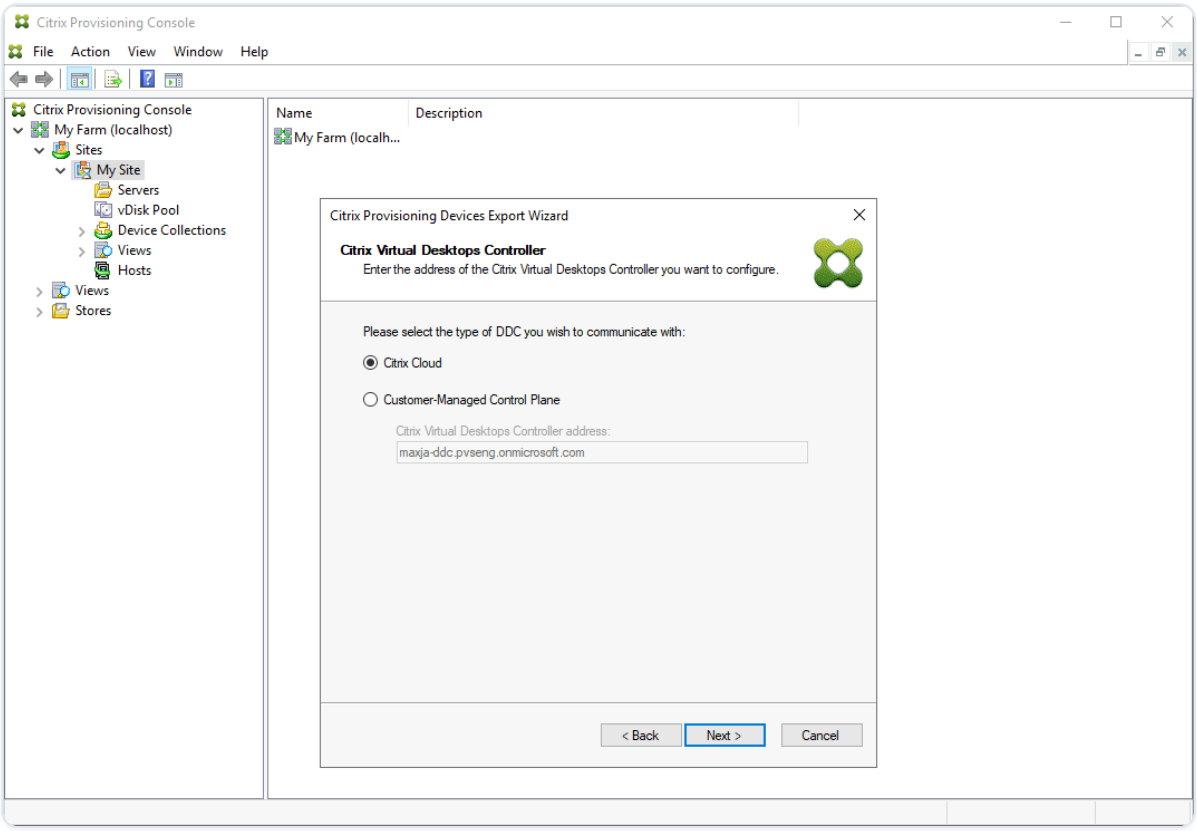
To add Citrix Provisioning managed VDAs to a machine catalog:

- Use the Citrix Virtual Apps and Desktops Setup Wizard in the Citrix Provisioning console

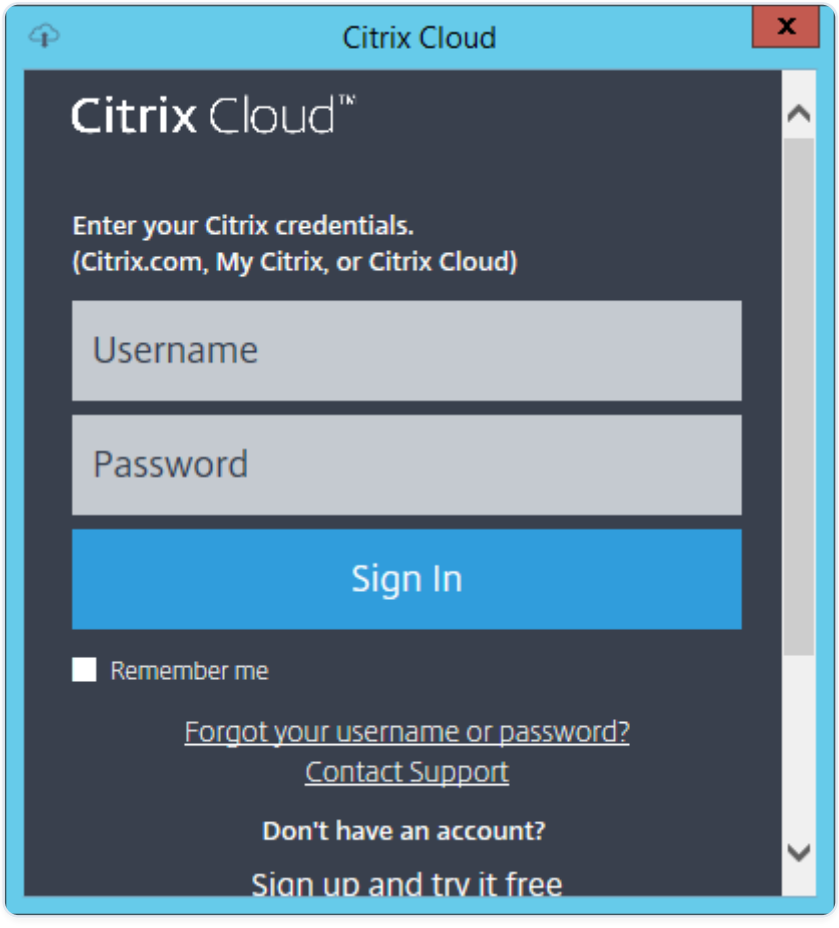
Using the Citrix Virtual Apps and Desktops Setup wizard to add VDAs

The Citrix Virtual Apps and Desktops Setup Wizard creates Citrix Provisioning devices and collections, then creates machine catalogs containing these elements.

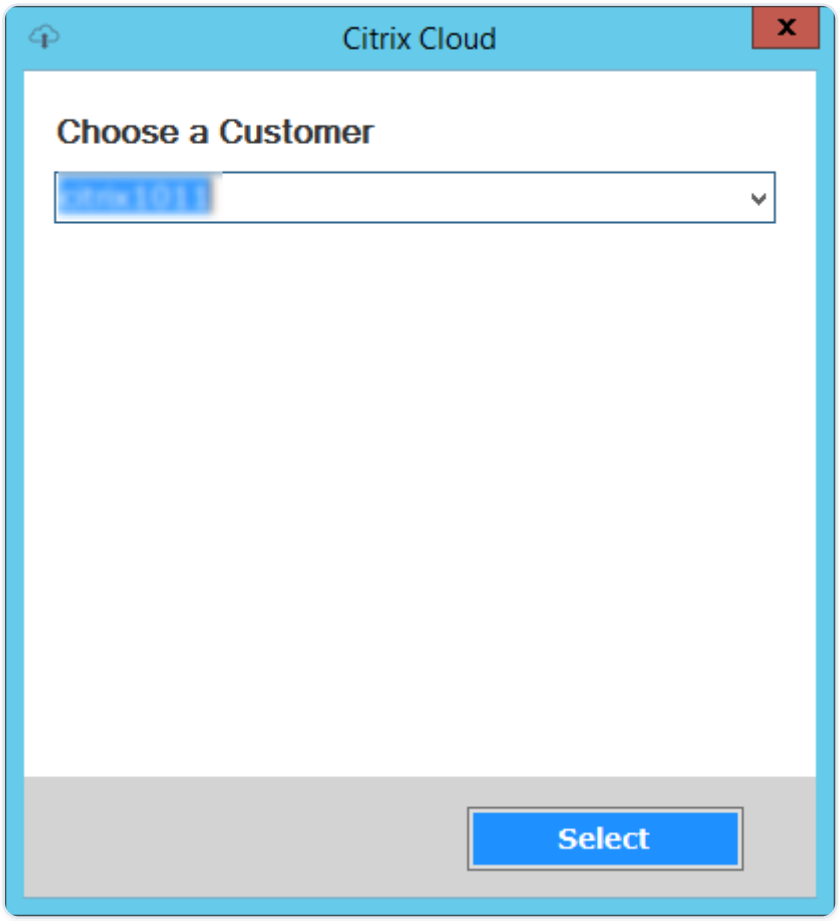
1. On the **Citrix Virtual Desktops™ Controller** page, select the type of Delivery Controller.
    a. If you select **Citrix Cloud**:



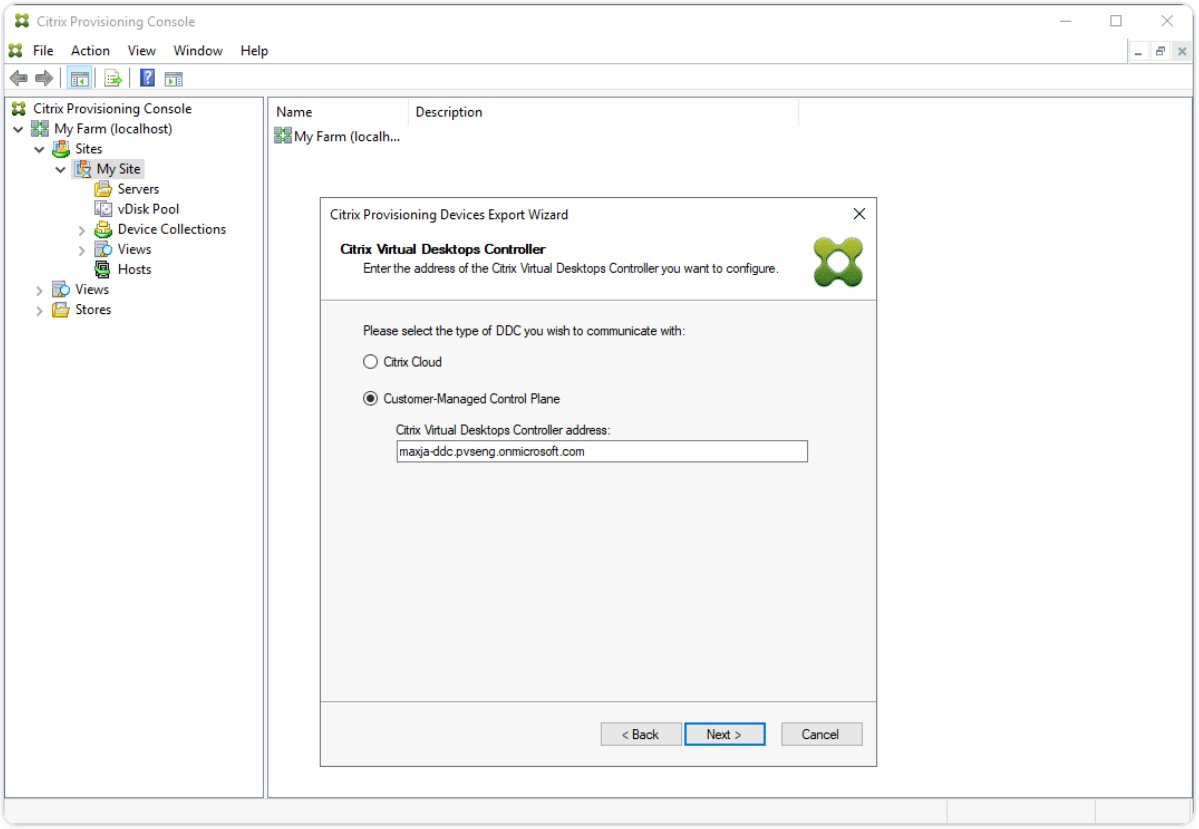
i. Enter your **Citrix Cloud credentials**. Click **Sign In**.



ii. After signing in to Citrix Cloud, select the appropriate cloud customer if requested.



b. If you select **Customer-Managed Control Plane**, enter the controller hostname or address. This authenticates using your current logged in user.



Troubleshooting

Use the information in this section to troubleshoot issues related to using the Citrix Virtual Apps and Desktops Setup Wizard for Delivery Controller connectivity.

- In Citrix Studio, ensure that the **Zones** screen properly displays the Cloud Connectors.
- Verify that at least one Cloud Connector is connected. To troubleshoot any issues with the Cloud Connector, see Troubleshooting.
- Ensure that the Citrix Provisioning console can make outgoing connections to the Delivery Controller. For more information on communication ports, see Tech Paper: Communication Ports Used by Citrix Technologies.

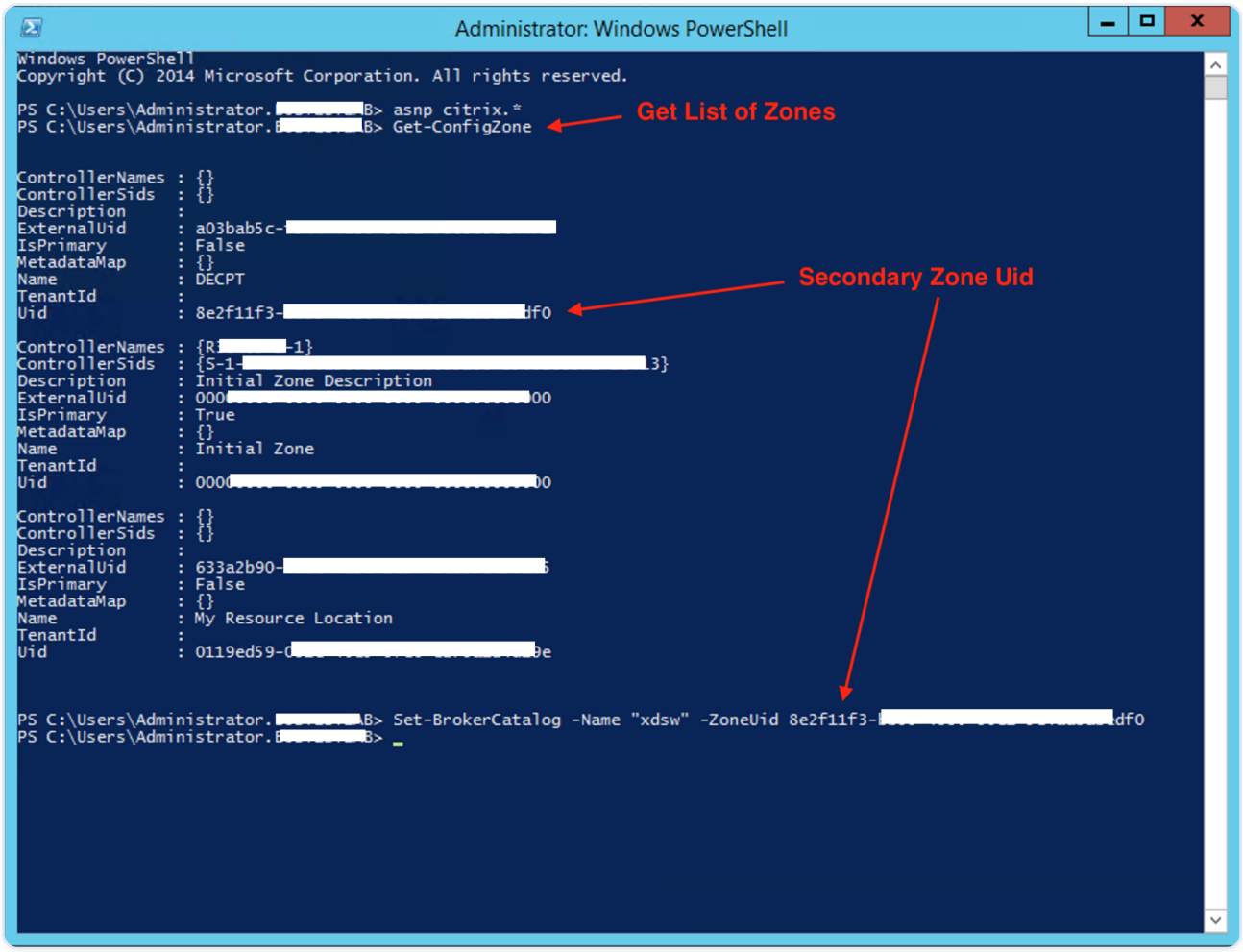
Support for multiple zones in the catalog creation process

Citrix Provisioning includes support for multiple zones in Citrix Virtual Apps and Desktops Setup and Export Devices wizards. In releases prior to version 1909, the wizards created catalogs and placed them in the Primary Zone by default. This behavior occurred for both the Citrix Cloud and On-premises Virtual Apps and Desktop DDC.

To correct the catalog locations and assign them to appropriate secondary zones, manually issue the Citrix Broker PowerShell cmdlet from the Citrix Provisioning™ console machine:

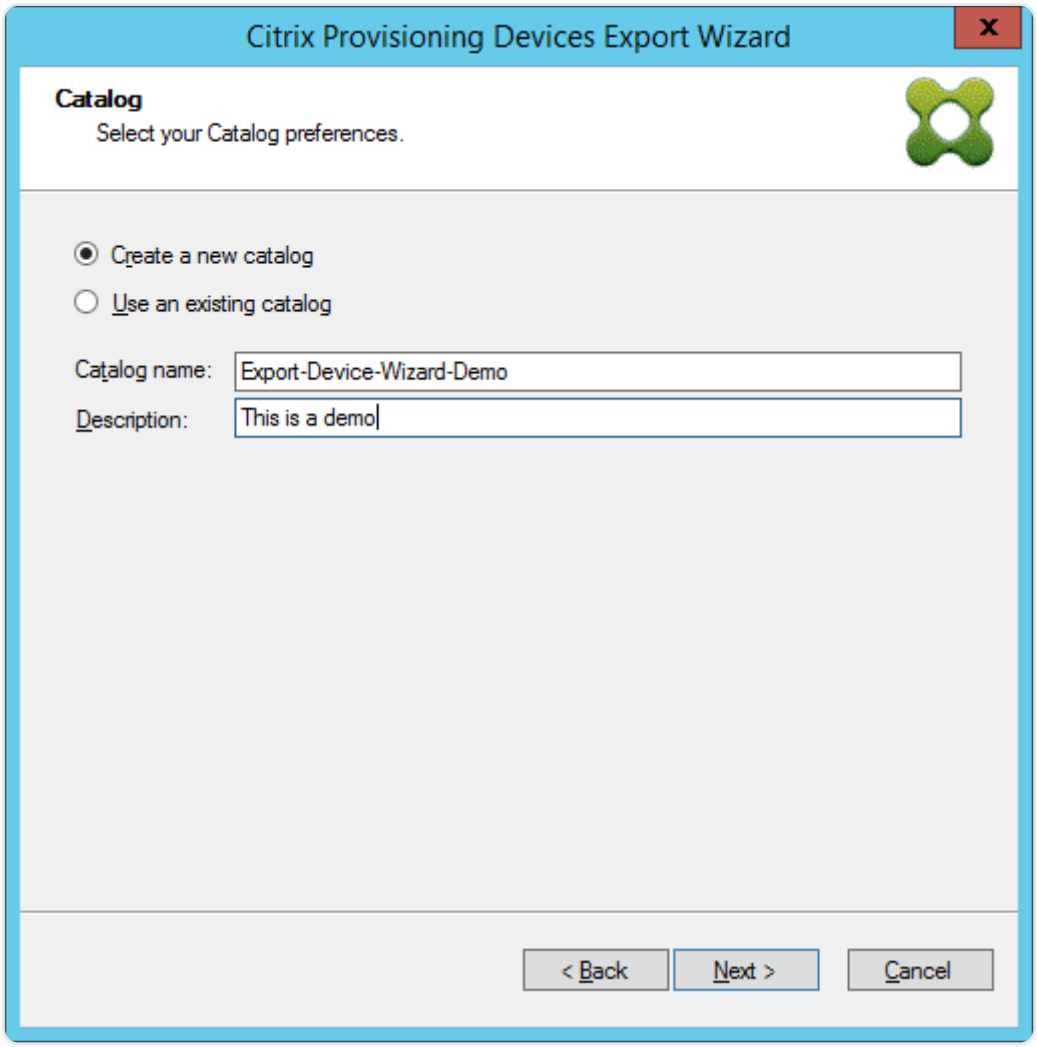
```
Set-BrokerCatalog-Name <CatalogName> -ZoneUid <GuidOfSecondaryZone>
```

The following image illustrates how a `Set-BrokerCatalog` PowerShell cmdlet was issued with the `-ZoneUid` parameter:



To correct the catalog locations and assign them to appropriate secondary zones, manually issue the Citrix Broker PowerShell cmdlet from the Citrix Provisioning console machine:

The following image illustrates the catalog preferences you can configure as part of both the Citrix Virtual Apps and Desktops™ wizard and the Citrix Provisioning Devices Export wizard. Instead of asking you to select a zone, both wizards automatically create the catalog in the zone of the hosting unit or hosting connection chosen in the earlier setup screen.



Provision target devices in untrusted domain using API PowerShell commands

You can provision target devices in an untrusted domain using Citrix Provisioning™ API PowerShell commands. Add the parameter `DomainCredentials` to the provisioning commands `Start-PvsProvisionMachines` and `Start-PvsProvisionXdMachines`.

The detailed steps are as follows:

1. Import Citrix Provisioning API PowerShell module.

   ```
   Import-Module "C:\Program Files\Citrix\Provisioning
   Services\Citrix.ProvisioningServices.dll"
   ```

2. Establish a connection to the Citrix Provisioning API server.

```
Set-PvsApiConnection -PvsServerAddress <server.domain> -PvsServerPort
54324 `

-Domain <domain> -Username <username>

-Password <password>
```

3. Input the credentials to create machine accounts in the untrusted domain.

```
$targetDeviceDomainCredentials = Get-Credential
```

4. Run `Start-PvsProvisionXdMachines` or `Start-PvsProvisionMachines` with the `DomainCredentials` parameter to provision target devices.

Note:

Run `Start-PvsProvisionXdMachines` if you want to provision VMs for XenDesktop® in the specified XenDesktop machine catalog.

- Provision XenDesktop machines: Example:

```
$provisionMachinesId = Start-PvsProvisionXdMachines `

-DdcAddress <your-ddc-address>`

-BootType <your-boot-type> `

-CatalogName <your-catalog-name> `

-CatalogDescription <your-catalog-description> `

-SessionSupport <your-session-support> `

-AllocationType <your-allocation-type> `

-PersistUserChanges <your-persist-user-changes> `

-Scope <your-scope>`
```

```
-VdaLevel <your-vda-level> `

-XenDesktopHostResource <your-xd-host-resource> `

-HostResourcePassword <your-host-resource-passsword> `

-TemplateName <your-template-name> `

-NetworkPath <your-network-path> `

-StoreId <your-store-id> `

-SiteId <your-site-id> `

-DiskLocatorId <your-disk-locator-id>`

-Domain <target-device-domain> `

-OrganizationalUnit <target-device-ou> `

-NamingScheme <your-naming-scheme> `

-VmCount <vm-count> `

-DeviceMemory <device-memory-size> `

-DeviceCpu <device-cpu-count> `

-DeviceWriteCacheSize <device-write-cache-size> `

-NameSuffixType <your-name-suffix-type> `

-CitrixCloud: <is-Citrix-Cloud> `

-DomainCredentials $targetDeviceDomainCredentials
```

- Provision VMs:

```
$provisionMachinesId = Start-PvsProvisionMachines `

-HostType <your-host-type> `
```

```
-HostAddress <your-host-address> `

-HostUsername <your-host-user-name> `

-HostPassword <your-host-password> `

-TemplateName <your-template-name> `

-StoreId <your-PVS-store-id> `

-SiteId <your-PVS-site-id> `

-CollectionId <your-collection-id> `

-DiskLocatorId <your-disk-locator-id> `

-Domain <target-device-domain> `

-OrganizationalUnit <target-device-ou>`

-NamingScheme <your-naming-scheme> `

-VmCount <vm-count> `

-DeviceMemory <device-memory-size> `

-DeviceCpu <device-cpu-count> `

-NameSuffixType <your-name-suffix-type> `

-DomainCredentials $targetDeviceDomainCredentials
```

5. Query the provisioning status repeatedly until the provisioning job is complete.

```
Get-PvsProvisioningStatus -ProvisionMachinesConnectionId
$provisionMachinesId
```

When provisioning of target devices in an untrusted domain is complete, you get the following output:

```
Cancelled : False

CurrentVmPercentComplete : 100

ErrorOccurred : False

Message : Machine Provisioning Complete!

OverallPercentComplete : 100
```

Create Citrix Provisioning™ catalogs in Citrix Studio

Currently, Citrix provides two provisioning solutions for creating VMs, Citrix Provisioning and Machine Creation Services™ (MCS).

To create a Citrix Provisioning catalog, you had to use the Citrix Virtual Apps and Desktops™ Setup Wizard. With this feature, you can now create a Citrix Provisioning catalog using Citrix Studio, Web Studio, and PowerShell commands.

This implementation provides you the following advantages:

- A single unified console to manage both MCS and Citrix Provisioning catalogs.
- Have new features for Citrix Provisioning catalogs, such as, identity management solution, on-demand provisioning and so on.

Currently, this feature is applicable to Azure, VMware, and XenServer.

> **Note:**
>
> This article is applicable to both DaaS and Citrix Virtual Apps™ and Desktops customers.

Considerations

- Image management is done using the existing Citrix Provisioning console.
- Only Boot Device Manager (BDM) is supported.
- While provisioning Citrix Provisioning target VMs, select the site for the target VMs. Ensure that the site is registered.

Limitations

Consider the following limitations for Azure:

- Gen 2 VMs are only supported.
- You can create a catalog using a machine profile. Do not enable hibernation in the machine profile input.
- You cannot set the following custom properties while creating the catalog:
  - StorageType
  - OsType
  - MachinesPerStorageAccount
  - StorageAccountsPerResourceGroup
  - UseSharedImageGallery
  - SharedImageGalleryReplicaRatio
  - SharedImageGalleryReplicaMaximum
  - UseEphemeralOsDisk
  - UseManagedDisks
  - StorageTypeAtShutdown

Consider the following limitation for VMware:

- Secure boot for the VM template is not supported. Therefore, do not select the **Secure Boot** check box under **Boot Options** in vSphere Client inventory.

Requirements

For Citrix Virtual Apps and Desktops on-premises users, following are the supported versions:

HYPERVISOR	CVAD RELEASE REQUIRED FOR STUDIO UI	CVAD RELEASE REQUIRED FOR POWERSHELL	SUPPORTED CITRIX PROVISIONING VERSION
Azure	2311 and later	2311 and later	2311 and later
VMware	2402 CU2 and later CUs of 2402 LTSR	2402 LTSR and later	2402 LTSR and later
XenServer	NA	2407 and later	2402 LTSR and later

Key steps

1. Set up Citrix Provisioning.
2. Join your farm with Citrix Cloud or Citrix Virtual Apps and Desktops site. See Join Citrix Cloud or Citrix Virtual Apps and Desktops site.
3. Create a master target device.
4. Create a vDisk using the Imaging Wizard. See Using the Imaging Wizard to create a virtual disk.
5. Add a connection to the hypervisor. See Citrix DaaS: Create and manage connections and resources and Citrix Virtual Apps and Desktops: Create and manage connections and resources.
6. Create a Citrix Provisioning catalog.
7. Check the collections in the Citrix Provisioning Console under **Sites**.

Create a Citrix Provisioning catalog using the Studio interface

> **Note:**
>
> See Requirements for supported release versions.
>
> If using Studio:

1. Sign in to Citrix Cloud.
2. In the left pane, select **Machine Catalogs**.

If using the Web Studio:

1. Sign in to Web Studio, select **Machine Catalogs** in the left pane.

To create a Citrix Provisioning catalog using Studio or Web Studio:

1. Select **Create Machine Catalog**. The catalog creation wizard opens.
2. On the **Machine Type** page, select a machine type for this catalog, such as **Multi-session OS** or **Single-session OS**.
3. On the **Machine Management** page, select the settings as follows:

a. Select **Machines that are power managed (for example, virtual machines or blade PCs)**.

b. Select **Citrix provisioning technology**. Then, select **Citrix Provisioning Services (PVS)**.

c. In the **Resources** field, select an Azure or VMware network resource for this catalog.

4. (Viewable only to single-session-OS catalogs) On the **Desktop Experience** page, select the random or static desktop experience as needed.
5. On the **Target Device** page, select the following:

   a. Select the farm and site for the machines to be provisioned.

   > **Note:**
   >
   > - The site field shows only sites registered with the Citrix Cloud.
   > - While you create a Citrix Provisioning catalog, on the **Target Device** page, you might see that in the drop-down menu to select the farm and site for the machines to be provisioned, there are farms and sites listed that no longer exist. As a workaround, you can run the PowerShell command `Unregister-HypPvsSite` to remove the farms and sites from the database. For information on the PowerShell command, see DaaS: Unregister-HypPvsSite and Citrix Virtual Apps and Desktops: Unregister-HypPvsSite.

   b. Select the vDisk to use with the provisioned machines.

   c. Select a machine profile for the provisioned machines.

6. On the **Storage and License Types** page, select the storage to use for this catalog and select the Windows volume licenses to provision VMs in Azure.
7. On the **Virtual Machines** page, select the count of VMs, VM size, and availability zone.

   For VMware environment, configure and enable the write-back-cache on the **Virtual Machines** page.
8. On the **NICs** page, add the NICs you want the VMs to use.
9. On the **Disk Settings** page, select the storage type and size of the write-back cache disk.

   > **Note:**

> This step is applicable for Azure environment only.

10. On the **Resource Group** page, choose whether to create resource groups or use existing groups. When you select **Create a resource group to provision machines**, a resource group is created with a name in the following format: `citrix-xd-<ProvSchemeId>-<Random5CharacterSuffix>`.

> **Note:**
>
> When you delete the catalog, the associated resource group is also deleted along with it.

11. On the **Machine Identities** page:
    a. Select an Identity type. For DaaS, you can select **Hybrid Azure Active Directory joined** for Azure and VMware environment.
    b. Select **Create new Active Directory accounts**. Specify an account naming scheme.
12. On the **Domain Credentials** page, click **Enter credentials**. Enter your domain credentials to perform account operations in the target Active Directory domain.
13. On the **Summary** page, enter a name for the machine catalog, and click **Finish**.

A Citrix Provisioning machine catalog is now created.

Create a customer-managed encryption key enabled catalog

You can create a Citrix Provisioning catalog enabled with customer-managed encryption key (CMEK) using the Studio UI and PowerShell commands in Azure environments.

You can create a machine-profile based catalog. The important considerations are:

- If there is a custom property or machine profile with DES Id, it always overrides the master image DES Id if they're different.
- If master image does not have DES Id, then DES Id in custom property overwrites DES Id value in the machine profile.
- You can change the DES Id of an existing catalog if the master image does not have DES Id. The new VMs only have the new DES Id.
- You can update an existing catalog to a CMEK enabled catalog.
- You cannot apply DES Id change to the existing VMs.

For more information on Azure Customer-managed encryption key, see Azure Customer-managed encryption key.

Create a Citrix Provisioning catalog using PowerShell commands

1. If you are not on the Citrix Provisioning server or on a system that has the Citrix Provisioning console installed, then download and install the latest Remote PowerShell SDK. For more information, see Install and use the Remote PowerShell SDK.
2. Open the **PowerShell** window.
3. Run the PowerShell commands to create a broker catalog and identity pool.

   Example in Azure:

   ```
   New-AcctIdentityPool -IdentityPoolName $catName -NamingScheme "$
   ($catName)##" -NamingSchemeType Numeric -Domain serenity.local
   ```

   Example in VMware:

   ```
   New-AcctIdentityPool `

   -IdentityPoolName $catName `

   -NamingScheme "$($catName)##" `

   -NamingSchemeType Numeric `

   -Domain $domain `

   -ZoneUid $zone.Uid
   ```

4. Run the `New-ProvScheme` command to create the catalog.

   Example in Azure:

   ```
   New-ProvScheme -AdminAddress "<address>" -CleanOnBoot `

   -ProvisioningSchemeType PVS `

   -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
   2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
   instance`">
   ```

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"OsType`"
Value=`"Windows`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"WBCDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"UseTempDiskForWBC`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"acbdpvs`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`" />

<Property xsi:type=`"StringProperty`" Name=`"Zones`" Value=`"1`" />

</CustomProperties>" `

-HostingUnitName "AzueRes"

-IdentityPoolName $catName `

-InitialBatchSizeHint 1 -LoggingId "854xxxxx-2xxx-42e0-
axxx-8c6xxx406xxx" `

-MachineProfile "XDHyp:
\HostingUnits\AzueRes\machineprofile.folder\abcdpvs.resourcegroup\abvda
```

```
.vm" `

-NetworkMapping @{"0"="XDHyp:\HostingUnits\AzueRes\
\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\abcdpvs.resourcegroup\fbgv-
vnet.virtualprivatecloud\default.network"} `

-ProvisioningSchemeName $catName `

-ServiceOffering "XDHyp:
\HostingUnits\AzueRes\serviceoffering.folder\Standard_D2s_v3.serviceoff
ering" `

-UseWriteBackCache -WriteBackCacheDiskSize 40 `

-PVSSite 6556cxxx-fc88-45f6-8xxx-ea4b665e9xxx -PVSvDisk cf056xxx-f69b-
xxxx-9a60-c41072b8xxxx
```

Example in VMware:

```
$ps = New-ProvScheme -CleanOnBoot  `

-ProvisioningSchemeType PVS `

-HostingUnitName $hostingUnit `

-IdentityPoolName $catName `

-MasterImageVM $machineProfile `

-ProvisioningSchemeName $catName `

-UseWriteBackCache -WriteBackCacheDiskSize 32

-PVSSite $pvsSite.SiteId `

-PVSvDisk $vDisk.DiskLocatorId
```

Example in XenServer:

```
$ps = New-ProvScheme -AdminAddress "<address>" -CleanOnBoot `

-ProvisioningSchemeType PVS `

-HostingUnitName "xen2" -IdentityPoolName   $catName `

-InitialBatchSizeHint 1 `

-VMCpuCount 2 `

-VMMemoryMB 8192 `

-NetworkMapping @{"0"="XDHyp:\HostingUnits\xen2\VM Network -
2607.network"} `

-ProvisioningSchemeName $catName `

-UseWriteBackCache -WriteBackCacheDiskSize 40 `

-PVSSite e9524976-8fc3-4ada-bf46-2156afdf4aa1 -PVSvDisk 22404f4e-
d65d-4072-abfe-161cbe7a952c `

-MasterImageVM "XDHyp:
\HostingUnits\xen2\pvstemplate.vm\pvs_template.snapshot"

$ps

Add-ProvSchemeControllerAddress -ProvisioningSchemeUid
$ps.ProvisioningSchemeUid -ControllerAddress @("W2K22ST-
U5DN1I0.serenity.local")
```

5. Create a broker catalog.

   Example in Azure:

   ```
   New-BrokerCatalog -AllocationType Random -Name $catName
   -PersistUserChanges Discard -ProvisioningType MCS -ProvisioningSchemeId
   $ps.ProvisioningSchemeUid -SessionSupport MultiSession
   ```

   Example in VMware:

```
New-BrokerCatalog `

-AllocationType Random `

-Name $catName `

-PersistUserChanges Discard `

-ProvisioningType MCS `

-ProvisioningSchemeId $ps.ProvisioningSchemeUid `

-SessionSupport MultiSession `

-MinimumFunctionalLevel L7_34
```

6. Add one VM to the catalog using the Studio UI or the following PowerShell command. Example:

```
$adId = New-AcctADAccount -Count 1 -IdentityPoolName $catName

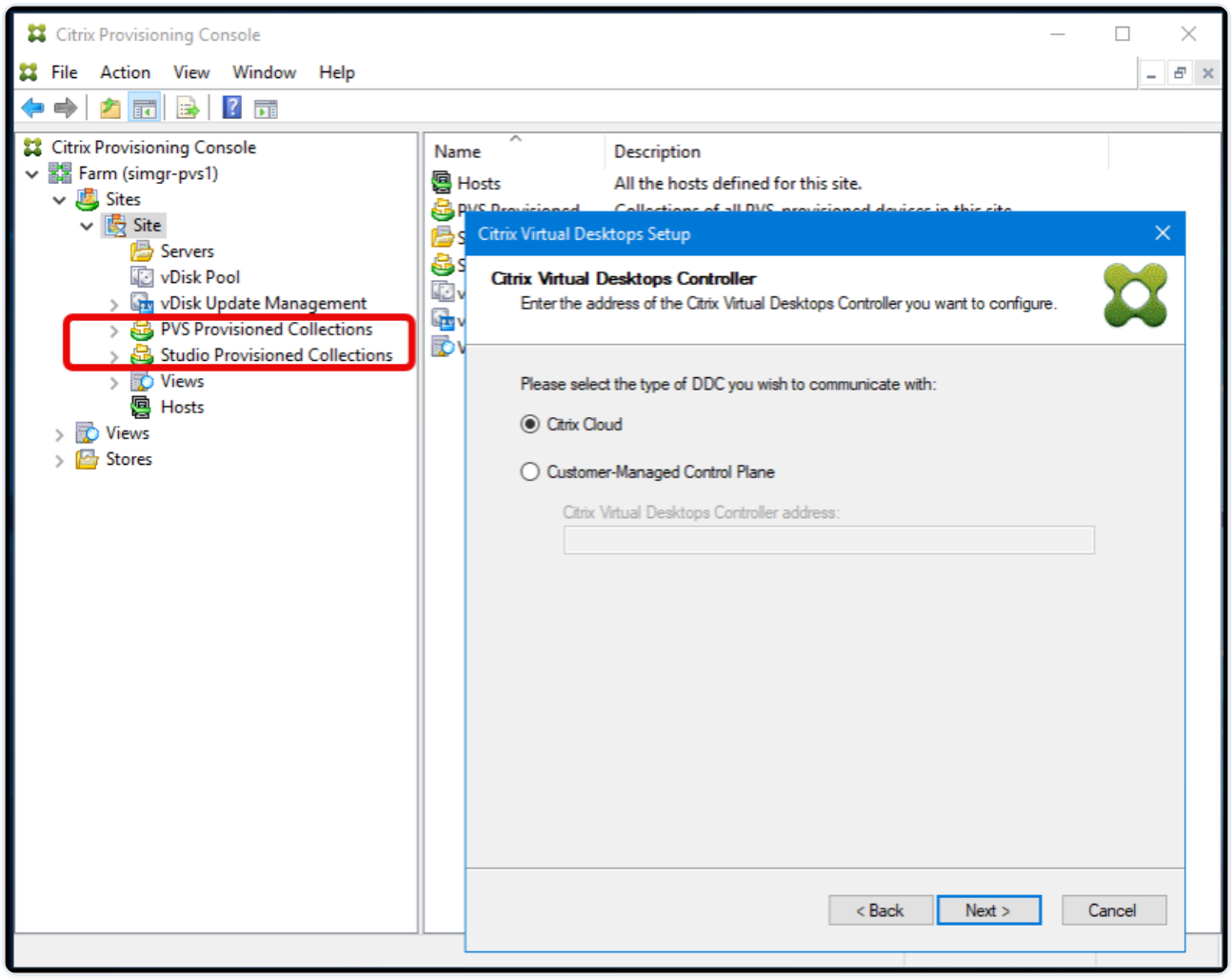
New-ProvVM -ProvisioningSchemeName $catName -ADAccountName
$adId.SuccessfulAccounts.ADAccountName
```

Check the collections in the Citrix Provisioning Console under Sites

After the Citrix Provisioning catalog is created, in the Citrix Provisioning console, you can see two types of collections under **Site** in the Citrix Provisioning console:

- **PVS Provisioned Collections**: All PVS-provisioned collections in the site
- **Studio Provisioned Collections**: All Studio-provisioned collections in the site

In the **Studio Provisioned Collections**, you can see collections with the same name as the Studio catalog.



Citrix Provisioning PowerShell SDK to get site and vDisk information

- To get the list of Citrix Provisioning sites where each site lists the Citrix Provisioning servers that are in that site, run the PowerShell command `Get-HypPvsSite`. For example:

```
Get-HypPvsSite -SiteId 00000000-0000-0000-0000-000000000000 -SiteName
"exampleSite" -FarmId 00000000-0000-0000-0000-000000000000 -FarmName
"exampleFarm" -ResourceLocation 00000000-0000-0000-0000-000000000000
```

> **Note:**
>
> All the parameters are optional in `Get-HypPvsSite` command. If you don't enter any parameters, you get the list of all the registered sites.

- To get a list of vDisks where each vDisk lists the site that it can be used with that vDisk, run the PowerShell command `Get-HypPvsDiskInfo`. For example, you can run one of the following:

- `Get-HypPvsDiskInfo -FarmId 00000000-0000-0000-0000-000000000000`
- `Get-HypPvsDiskInfo -SiteId 00000000-0000-0000-0000-000000000000 -StoreId 00000000-0000-0000-0000-000000000000`
- `Get-HypPvsDiskInfo -SiteId 00000000-0000-0000-0000-000000000000 -DiskLocatorId 00000000-0000-0000-0000-000000000000`

> **Note:**
>
> The command queries `FarmId` from registered sites using `SiteId` when no `FarmId` is given.

Create Hybrid Azure AD joined catalogs

You can create a Hybrid Azure AD joined catalog using one of the following:

- The Citrix Virtual Desktops™ Setup Wizard in Citrix Provisioning Console.
- Studio UI or PowerShell commands.

This article describes how to create a Hybrid Azure AD joined catalog using the two different ways.

> **Note:**
>
> This article is applicable to both DaaS and Citrix Virtual Apps and Desktops™ customers.

Key Steps

1. Set up a Hybrid Azure AD environment.
2. Set up Citrix Provisioning™ server.
3. Join your farm with Citrix Cloud or Citrix Virtual Apps™ and Desktops site: when using the Studio UI or PowerShell.
4. Create a master target device.
5. Run the Imaging Wizard to create a vDisk.
6. Create a Hybrid Azure AD joined catalog.

Set up Hybrid Azure AD environment

Set up Hybrid Azure AD and enable Microsoft Entra Connect Sync on the Domain Controller. For information, see Configure Microsoft Entra hybrid join.

Set up Citrix Provisioning

To set up Citrix Provisioning, begin by configuring your provisioning server and other infrastructure. See Install Citrix Provisioning software components.

Join your farm with Citrix Cloud™ or Citrix Virtual Apps and Desktops site

If you want to create a Hybrid Azure AD joined catalog using the Studio UI or PowerShell, then run the Configuration Wizard to join the Citrix Provisioning servers in a farm to Citrix Cloud or Citrix Virtual Apps and Desktops site.

See Join Citrix Cloud or Citrix Virtual Apps and Desktops site.

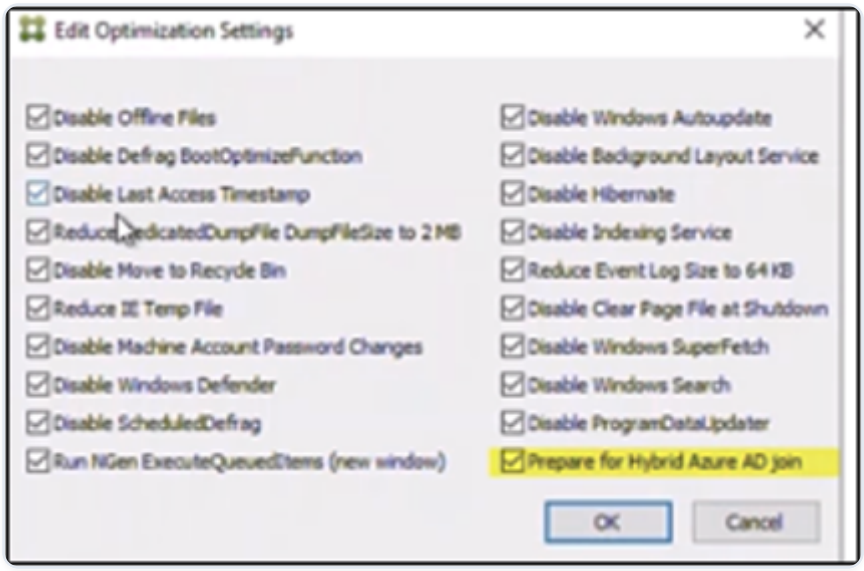
Create a master target device

1. Create a master target device.
2. Run the command `dsregcmd /leave` to leave the master target device from Hybrid Azure AD joined.

Run Imaging Wizard to create a vDisk

Use the Imaging Wizard to create the vDisk from the master target device. For more information, see Using the Imaging Wizard to create a virtual disk.

While running the Image Wizard to create a vDisk, select **Prepare for Hybrid Azure AD join** in the **Edit Optimization Settings** dialog if you want to create a Hybrid Azure AD joined catalog.



Create a Hybrid Azure AD joined catalog

You can create a Citrix Provisioning Hybrid Azure AD joined catalog using one of the following:

- The Citrix Virtual Desktops Setup Wizard in Citrix Provisioning Console.
- MCS provisioning (Studio UI or PowerShell commands).

Using Citrix Virtual Desktops Setup Wizard

1. For information on how to create target devices using Citrix Virtual Desktops Setup Wizard, see Deploying virtual desktops to VMs using the Citrix Virtual Apps and Desktops Setup Wizard.
2. After the target devices are created, see the Citrix Provisioning catalog on the Full configuration interface.
3. Complete creating delivery groups.
4. After approximately 90 minutes, locate the delivery group in the Delivery Group list, and check the **Details** tab. When the target devices complete Hybrid Azure AD join, the value of the **Unregistered Machines** must be **zero**.

> **Note:**

> The joining time can vary. However, the target devices must join within 90 minutes.

Using MCS provisioning

> **Note:**

This option is available from CVAD 2402 LTSR CU3 or later

You can use the Studio UI or PowerShell commands to create a Citrix Provisioning Hybrid Azure AD joined catalog. If you use Studio provisioning, then target devices join Hybrid Azure AD immediately.

Currently, Azure and VMware hypervisors are supported.

For Citrix Virtual Apps and Desktops on-premises users, following are the supported versions:

HYPERVISOR	CVAD RELEASE REQUIRED FOR STUDIO UI	CVAD RELEASE REQUIRED FOR POWERSHELL	SUPPORTED CITRIX PROVISIONING VERSION
Azure	NA	2311 and later	2311 and later
VMware	NA	2402 LTSR and later	2402 LTSR and later

Note:

You can currently create the Citrix Provisioning Hybrid Azure AD joined catalog using:

- Studio and PowerShell in DaaS.
- Only PowerShell commands in Citrix Virtual Apps and Desktops.

Using the Studio UI

For information on creating a machine catalog using the Studio UI interface, see Create a Citrix Provisioning catalog using the Citrix Studio interface.

On the **Machine Identities** page, select **Hybrid Azure Active Directory joined**.

Note:

The **Hybrid Azure Active Directory joined** option is now available for Citrix Virtual Apps and Desktops customers from 2402 LTSR CU3.

Using PowerShell

Do the following steps to create the catalog using PowerShell commands:

1. Create Hybrid Azure AD Identity Pool using `New-AcctIdentityPool` command.

> **Note:**
>
> When creating the identity pool, make sure the specified Domain and Organizational Unit (OU) are the same as the ones you created when setting up the Hybrid Azure AD environment.

1. Create AD Accounts using the `New-AcctADAccount` command.
2. Set `userCertificate` for AD Accounts using `Set-AcctAdAccountUserCert` command.
3. Create a provisioning scheme using the `New-ProvScheme` command.
4. Create a broker catalog using the `New-BrokerCatalog` command.
5. You can add VMs to the catalog using **Full Configuration interface > Machine Catalogs**. Alternatively, you can use the PowerShell command `New-ProvVmNew-BrokerMachine`.

Example: This is a sample script for the same enhancement used for Citrix Provisioning on Azure. However, the steps are similar when Citrix Provisioning runs on VMware.

```
asnp citrix*

# General variable settings

$ipName = "ip-ex"

$domainPrefix = "abcdef"

$domainExtension = "com"

$ou = "mixxxx-haad"

$username = "username"

$password = "password"
```

```
# ProvScheme configurations

$provSchemeName = "haad-ex"

$hostingUnit = "hosting unit"

$resourceGroup= "mixxxx"

$machineProfile = "XDHyp:\HostingUnits\$hostingUnit\machineprofile.folder\
$resourceGroup.resourcegroup\mixxxx
-standard.templatespec\v1.templatespecversion"

$serviceOffering = "XDHyp:\HostingUnits\
$hostingUnit\serviceoffering.folder\Standard_D2s_v3.serviceoffering"

$networkMapping = @{"0"=“XDHyp:\HostingUnits\
$hostingUnit\virtualprivatecloud.folder\
$resourceGroup.resourcegroup\mixxxx-
vnet.virtualprivatecloud\default.network"}

# PVS settings

$pvsFarmName = "mixxxx-farm"

$pvsSiteName = "mixxxx-site"

$pvsDiskName = "pvs-vda-haad"

# Basic PVS objects

$pvsSite = Get-HypPvsSite -SiteName $pvsSiteName -FarmName $pvsFarmName

$vDisk = Get-HypPvsDiskInfo -SiteId $pvsSite.SiteId | ?
{ $_.DiskLocatorName -eq "$pvsDiskName" }

$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PersistWBC" Value="True" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
```

```
Value="$resourceGroup" />

</CustomProperties>

"@

# 1. Create a IdentityPool

New-AcctIdentityPool `

  -IdentityPoolName $ipName `

  -IdentityType HybridAzureAD `

  -NamingScheme "$($provSchemeName)##" `

  -NamingSchemeType Numeric `

  -Domain "$domainPrefix.$domainExtension" `

  -OU "OU=$ou,DC=$domainPrefix,DC=$domainExtension"

# 2. Create ADAccounts

$password = ConvertTo-SecureString $password -AsPlainText -Force

New-AcctADAccount `

  -IdentityPoolName $ipName `

  -Count 1 `

  -StartCount 1 `

  -ADUserName $username `

  -ADPassword $password `

  -OutVariable result

# 3. Set ADAccount userCertificate

Set-AcctAdAccountUserCert `
```

```
  -IdentityPoolName $ipName `

  -ADUserName "$domainPrefix\$username" `

  -ADPassword $password `

  -All

# 4. Create a ProvScheme

$ps = New-ProvScheme -CleanOnBoot `

  -ProvisioningSchemeName $provSchemeName `

  -HostingUnitName $hostingUnit `

  -IdentityPoolName $ipName `

  -MachineProfile $machineProfile `

  -ServiceOffering $serviceOffering `

  -NetworkMapping $networkMapping `

  -PVSSite $pvsSite.SiteId `

  -PVSvDisk $vDisk.DiskLocatorId `

  -ProvisioningSchemeType PVS `

  -UseWriteBackCache -WriteBackCacheDiskSize 127 -WriteBackCacheMemorySize
256 `

  -CustomProperties $customProperties

# 5. Create a Broker Catalog

New-BrokerCatalog `

  -AllocationType Random `

  -Name $provSchemeName `
```

```
    -PersistUserChanges Discard `
    -ProvisioningType "MCS" `
    -SessionSupport SingleSession `
    -ProvisioningSchemeId $ps.ProvisioningSchemeUid
```

Manage

Use the information in this section to manage Citrix Provisioning™:

- Farms represent the top level of a Citrix Provisioning infrastructure.
- Sites provide a method of representing and managing logical groupings of Citrix Provisioning servers, device collections, and local shared storage.
- Servers to stream software from vDisks, as needed, to target devices.
- Stores represent the logical name for the physical location of the virtual disk folder.
- Device collections to create and manage logical groups of target devices.
- Target devices represent desktops, servers, or any other component that gets software from a virtual disk on the network.
- vDisks are streamed to target devices by the Provisioning Server.
- Views used to manage a group of target devices.

Farms

A farm represents the top level of a Citrix Provisioning™ infrastructure. Farms provide a method of representing, defining, and managing logical groups of provisioning components into sites.

All sites within a farm share that farm's Microsoft SQL database. A farm also includes a Citrix License Server, local or network shared storage, and collections of target devices.

The farm is initially configured when you run the Configuration Wizard. The wizard prompts you for the farm's name, a store, and a device collection. When you first open the Citrix Provisioning console, those objects display in the tree.

The wizard prompts you for more farm information. Such as the name of the license server, your user account information, and those servers serving the bootstrap file to target devices. You can always rerun the wizard to change settings, or choose to make farm configuration changes using the Farm Properties Dialog.

A farm administrator can view and manage all objects in any farm to which they have privileges. Only farm administrators can perform all tasks at the farm level.

Connecting to a farm

1. Right-click on a console in the navigation tree, then select **Connect to farm**.
2. In the **Server Information** field, type the name or IP address of a streaming server on the farm and the port configured for server access.
3. Select to log in using one of the following methods:
    - Use your current Windows login credentials, then optionally enable the **auto-login on application start or reconnect** feature.
    - Use different Windows credentials by entering the user name, password, and domain associated with those credentials. Optionally enable the **Save password** and **auto-login on application start or reconnect** feature.
4. Click **Connect**. The **Farm** icon appears in the console.

Managing connections

You can manage connections to farms from the **Manage Connections** dialog box. To open the dialog, right-click on the Citrix Provisioning console icon in the tree, then select the **Manage Connections** menu option.

Sites

A site allows you to manage logical groupings of Citrix Provisioning™ servers, device collections, and local shared storage. A site administrator can perform any task that a device administrator or device operator within the same farm can perform.

A site administrator can also perform the following tasks:

Farm-level tasks:

- Managing site properties, as described in this article: Managing Stores

Some site-level tasks include:

- Defining device administrator and device operator roles.
- Managing provisioning servers
- Managing connections
- Creating a site in a farm, as described in this article: Rebalancing devices on the provisioning server

- Importing target devices into collections
- Accessing auditing information

To create a site:

1. Right-click on the sites folder in the farm where you want to add the new site. The **Site Properties** dialog appears.
2. On the **General** tab, type the name and a description for the site in the appropriate text boxes.
3. On the **Security** tab, click **Add** to add security groups that have the site administrator rights in this site. The **Add Security Group** dialog appears.
4. Select the group to which you want to apply site administrator privilege, then click **OK**. Optionally, check the **Domains/Group Name** check box to select all groups in the list.
5. On the **Options** tab, if new target devices are to be added using the **Auto-Add** feature, select the collection where these target devices reside. Enable this feature first in the **Farm** properties dialog.

To modify an existing site's properties, right-click on the site in the Citrix Provisioning console, then select **Properties**. Make modifications in the **Site Properties** dialog. The tabs in this dialog allow you to configure a site. Site administrators can also edit the properties of a site that they administer.

The **Site Properties** dialog contains the following tabs.

General Tab:

- **Name:** Type the name of this site in the textbox.
- **Description:** Optional. Type the description of this site in the textbox.

Security Tab:

- **Add:** Click **Add** to open the **Add Security Groups** dialog. Select the group to which you want to apply site administrator privilege. To add all groups that are listed, check the **Domain\Group Name** check box.
- **Remove:** Click *Remove* to remove site administrator read-only privileges of the selected groups. To remove all groups that are listed, check the **Domain\Group Name** check box.

MAK Tab:

- **Enter the administrator credentials used for Multiple Activation Key enabled Devices:** MAK administrator credentials must be entered before target devices using MAK can be activated. The user must have administrator rights on all target devices that use MAK enabled vDisks and on all provisioning servers that stream those target devices. After entering the following information, click **OK**:
  - User
  - Password

> **Note:**
>
> If credentials have not been entered and an activation attempt is made from the **Manage MAK Activations** dialog, an error message displays. The **MAK** tab appears, allowing you to enter the credential information. After entering credentials, click **OK** and the **Manage MAK Activations** dialog reappears.

Options Tab:

- **Auto-Add:** Select the collection for the new target device from the menu. Enable this feature first in the **Farm** properties dialog. Set the number of seconds to wait before Citrix Provisioning scans for new devices specified in the **Seconds between inventory scans** option. The default is 60 seconds.

vDisk Update Tab:

- **Enable automatic vDisk updates on this site:** Select this check box to enable automatic vDisks updates, then select the server running the updates for this site.

Servers

A Citrix Provisioning™ server is any server that has stream services installed. Provisioning servers are used to stream software from virtual disks, as needed, to target devices. In some implementations, these disks reside directly on the provisioning server, and in other environments, provisioning servers get the virtual disk from a shared storage device.

Provisioning servers also retrieve and provide configuration information to and from the Citrix Provisioning database. Configuration options are available to ensure high availability and load-balancing of target device connections.

To configure a provisioning server and software components for the first time, run the Configuration Wizard. The Configuration Wizard can be rerun on a provisioning server later to change network configuration settings.

After the server components are installed, they are managed using the Citrix Provisioning console.

> **Tip:**
>
> When configuring provisioning servers, ensure that proper firewall isolation is observed so that the deployment provides a robust security boundary around all servers. Extend this isolation to the SQL server and disk storage, so that network access outside the security boundary is restricted. This configuration prevents viewing of weakly authenticated or unencrypted data flows.
>
> At a minimum, isolate only those server instances that communicate with one another on their unauthenticated intra server communication channels. To isolate server instances, configure hardware firewalls to ensure that packets cannot be routed from outside this boundary to servers within the boundary. Extend this firewall protection paradigm to the SQL server and disk storage components where configurations do not have appropriate SQL server and disk storage links. Extending the firewall prevents unauthorized users from targeting these additional components.

Provisioning servers in the console

A provisioning server is any server that has Stream Services installed. These servers are used to stream software from vDisks, as needed, to target devices. In some implementations, vDisks reside directly on the provisioning server. In larger implementations, servers get the virtual disk from a shared-storage device on the network.

The Citrix Provisioning console is used to perform provisioning server management tasks such as editing the configuration settings or the properties of existing provisioning servers.

Servers appear in the console main window as members of a site within a farm. To manage servers that belong to a specific site, you must have the appropriate administrative role. These roles include site administrator for this site, or the farm administrator.

> **Note:**

> In the console, the appearance of the provisioning server icon indicates that server's status.

> In the console, provisioning servers are managed by performing actions on them. To view a list of actions that can be performed on a selected server, choose from the following options:

- Click the **Action** menu in the menu bar.
- Right-click on a **provisioning server** in the console.
- Enable the **Action** pane from the **Views** menu.

> **Note:**
>
> Actions appear disabled if they do not apply to the selected provisioning server. See *Management Tasks* for task details.

Showing Citrix Provisioning server connections

To view and manage all target device connections to the provisioning server:

1. Highlight a provisioning server in the console. Select **Show connected devices** from the **Action** menu, right-click menu, or **Action** pane. The **Connected Target Devices** dialog appears.

   > **Note:**
   >
   > The IPv6 address is displayed in the device IP column for targets using IPv6.

2. Select one or more target devices in the table to perform any of the following connection tasks:

   |Option|Description| | -- | -- | |Shutdown|Shuts down target devices that are highlighted in the dialog.| |Reboot|Reboots target devices that are highlighted in the dialog.| |Message|Opens the **Edit Message** dialog to allow you to type, and then send a message to target devices highlighted in the dialog.|

   > **Note:**

> When selecting **Shutdown** or **Reboot**, a dialog opens providing the option to type a message that displays on the affected devices. The **Shutdown** or **Reboot** options can be delayed by entering a delay time setting.

> If a message confirms that the target device was successfully shut down or rebooted, but the icon in the console window does not change, select the **Refresh** button.

Balancing the target device load on provisioning servers

To achieve optimum server and target device performance within a highly available network configuration, enable load balancing for each virtual disk.

1. Right-click on the **vDisk** in the console, then select the **Load Balancing** menu option. The **vDisk Load Balancing** dialog box appears. For details, see Servers.
2. After enabling load balancing for the virtual disk, set the following extra load balancing algorithm customizations:

    - Subnet Affinity – When assigning the server and NIC combination to use to provide this virtual disk to target devices, select from the following subnet settings:

        - None – ignore subnets. Uses the least busy server. None is the default setting.
        - Best Effort – use the least busy server/NIC combination from within the same subnet. If no server/NIC combination is available within the subnet, select the least busy server from outside the subnet. If more than one server is available within the selected subnet, perform load balancing between those servers.
        - Fixed – use the least busy server/NIC combination from within the same subnet. Perform load balancing between servers within that subnet. If no server/NIC combination exists in the same subnet, do not boot target devices assigned to this virtual disk.

    - Rebalance Enabled using Trigger Percent – Enable this option to rebalance the number of target devices on each server when the trigger percent is exceeded. When enabled, Citrix Provisioning checks the trigger percent on each server approximately every 10 minutes. For example: If the trigger percent on this virtual disk is set to 25%, rebalancing occurs within 10 minutes if this server has 25% more load in comparison to other servers that can provide this virtual disk.

> **Note:**

The load balance algorithm considers the Server power setting of each server when determining load.

Load balancing fails if:

- Less than five target devices are using a particular server.
- The average number of target devices using all qualifying servers is less than five.
- The number of target devices that are booting on a given server is more than 20% of the total number of devices connected to the server. This configuration prevents load shift thrashing during a boot storm.

Load balancing is also considered when a target device boots. Citrix Provisioning determines which qualified provisioning server, with the least amount of load, provides the virtual disk. Whenever more qualified servers are brought online, rebalancing occurs automatically.

To implement load balancing in a high availability network configuration

- Assign a power rating to each provisioning server on the Server properties' General tab.
- For each virtual disk, select the load balancing method and define any additional load balancing algorithm settings on the **vDisk Load Balancing** dialog box. For details, see Servers.

Note:

Target devices that not using a virtual disk in high availability mode are not diverted to a different server. If a virtual disk is misconfigured to have high availability enabled, but they are not using a valid high availability configuration. Provisioning servers, stores and target devices that use that virtual disk can lock up.

To rebalance provisioning server connections manually

1. In the Citrix Provisioning console, highlight the provisioning servers to rebalance, right-click then select the **Rebalance devices** menu option. The **Rebalance Devices** dialog appears.
2. Click **Rebalance**. A rebalance results message displays under the **Status** column.
3. Click **Close** to exit the dialog.

Checking for provisioning server virtual disk access updates

To check for updates to vDisks that the selected provisioning server accesses:

1. Right-click the provisioning server in the **Details** pane, then select **Check for updates**.
2. Select the **Automatic...** menu option.
3. Click **OK** on the confirmation message that appears. The virtual disk is automatically updated or is scheduled for an update.

Disabling write cache to improve performance when using storage device drives

Disable write caching to improve the performance when writing from a provisioning server to storage device drives such as an IDE or SATA drive.

In Windows, to disable write caching on the server hard drive for the storage device on which your vDisks are stored:

1. On the provisioning server, open the **Control Panel**. Select **Administrative Tools>Computer Management**.
2. Double-click the **Disk Management** node in the tree.
3. Right-click the storage device for which Windows write caching is disabled.
4. Select **Properties**, then click the **Hardware** tab.
5. Click the **Properties** button.
6. Click the **Policies** tab.
7. Clear the **Enable write caching on the disk** check box.
8. Click **OK**, then click **OK** again.
9. Close the **Computer Management** window, then the **Administrative Tools** window.
10. Right-click the provisioning server node in the console, then click **Restart service**. Alternatively, you can also rerun the Configuration Wizard to restart the services, or manually restart the services through the **Windows Control Panel>Administrative Tools>Services** window. At the **Services** window, right-click on the Stream Service, then select **Start** from the shortcut menu.

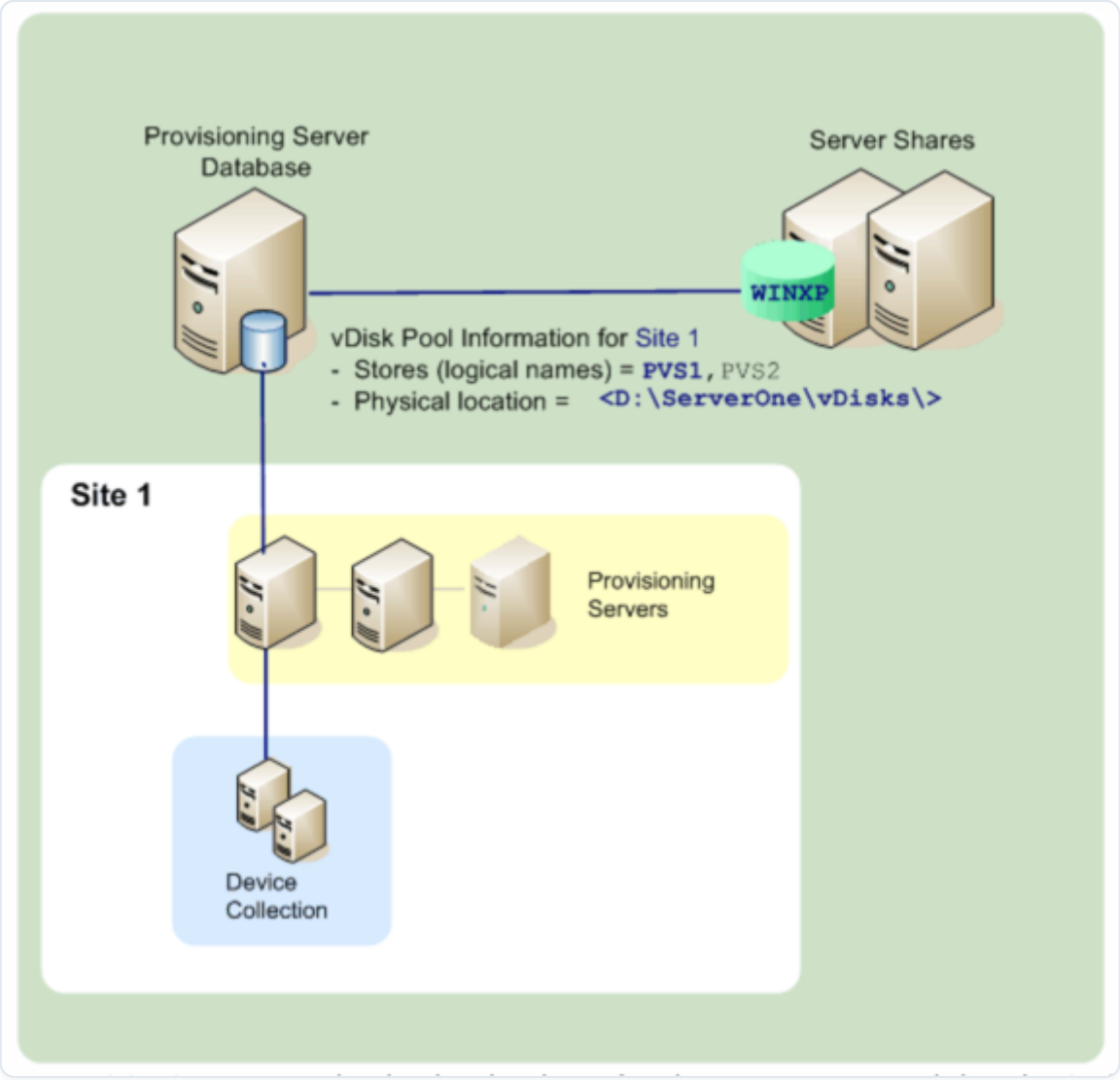
Providing provisioning servers with access to stores

For each store, select the provisioning servers that can access that store:

1. In the Citrix Provisioning console, right-click on the **Store**, then select the **Properties** menu option. The **Store Properties** dialog appears.
2. On the **Servers** tab, select the site where provisioning servers access this store.
3. Enable the check box next to each provisioning server that can provide vDisks in this store, then click **OK**.

Stores

A store is the logical name for the physical location of the virtual disk folder. This folder can exist on a local server or on a shared storage device. When virtual disk files are created in the Citrix Provisioning™ console, they are assigned to a store. Within a site, one or more Citrix Provisioning servers are given permission to access that store to serve virtual disks to target devices.



A provisioning server checks the database for the store name and the physical location where the virtual disk resides, then provides it to the target device.

Separating the physical paths to a virtual disk storage location allows for greater flexibility within a farm configuration. Particularly if the farm is configured to be highly available. In a highly available implementation, if the active provisioning server in a site fails, the target device can get its virtual disk from another server that has access to the store and permissions to serve it.

If necessary, copies of virtual disks are maintained on a secondary shared storage location if that connection to the primary shared storage location is lost. In this case, the default path is set in the store properties if all provisioning servers can use the same path to access the store. If a particular server cannot use the path then an override path can be set in the store properties for that particular server. Use an override path when the default path is not valid for that server. This does not occur because of a connection loss, but because the path is not valid. Provisioning servers always use the default path if the override path does not exist in the database.

Store administrative privileges

Stores are defined and managed at the farm level by a farm administrator. Access or visibility to a store depends on the users administrative privileges:

- Farm administrators have full access to all stores within the farm.
- Site administrators have access to only those stores owned by the site.
- Device administrators and device operators have read-only access. Site administrators also have read-only access if that store exists at the farm level, or if that store belongs to another site.

Creating a store

1. In the Citrix Provisioning console tree, right-click on **Stores**, then select the **Create store** menu option. The **Store Properties** dialog appears.
2. On the **General** tab, type the store name and a description of this store. The store name is the logical name for this storage location.
3. Optionally, select the site that acts as the owner of this store. Otherwise, accept the default \<None> so that only farm administrators can manage this store.
4. On the **Servers** tab, select a site from the list. All provisioning servers in that site appear.
5. Check the box next to each server that is permitted to access this store. If the store is only for a specific site, only those servers within that site are valid selections. Also, if the default path is not valid for a selected server, an override path must be defined for that server on the **Server Properties** dialogs **Store** tab. Repeat this step for each site if necessary. If the site administrator performs this procedure, only those sites that they administer appear.

6. On the **Paths** dialog, type or browse for the default path for this store. The path represents the physical location of the virtual disk folder. Optionally, a new folder can be created by clicking the **Browse** button, and then clicking **Create New Folder**. If the user is a site administrator, only those sites that they administer are available in the list.
7. The write cache path for the selected store display under the paths list. Optionally, a new store cache folder can be created by clicking the **Browse** button, and then clicking **Create New Folder**. More write cache paths can be added for use by the store by clicking **Add**. Entering more than one write cache paths allows for virtual disk load to be distributed to physically different drives. When a target device first connects, the Stream Service picks from the list. When using high availability, the order of the write-cache paths for any override paths in store properties for that server must match. The order of the write-cache paths specified must be the same.

   If a write cache path is not selected and the **OK** button is clicked, the user is prompted to create the default write cache path. Click **OK** on this message to create the default write cache path, `C:\pvsstore\WriteCache`.
8. After configuring the store and paths used by the store, click **Validate** to open the **Validate Store Paths** dialog and validate the path settings.
9. Under the **Status** column, view the path validation results. Click **Close** to close this dialog and return to the **Store Properties** dialog to make any necessary changes or to continue.
10. Click **OK** to save property settings.

Store properties

Create a store by running the Configuration Wizard or in the **Store Properties** dialog. The store properties dialog allows you to:

- name and provide a description of the store.
- select the owner of the store, the site which manages the store.
- provide a default path to the store, the physical path to the virtual disk.
- define default write cache paths for this store.
- select the servers that can provide this store.

After a store is created, store information is saved in the Citrix Provisioning database. Each site has one virtual disk pool, which is a collection of virtual disk information required by Citrix Provisioning servers that provide vDisks in that site. The virtual disk information can be added to

the virtual disk pool using the **vDisk Properties** dialog or by scanning a store for new vDisks that have not yet been added to the database.

The **Store Properties** dialog includes the following tabs:

General:

- **Name:**
  - View, type the logical name for this store. For example, *Provisioning-1*.
  - View or type a description of this store.
- **Description:** View or type a description for this store.
- **Site that acts as owner of this store:** Optional. View or scroll to select the site that acts as owner of this store. This feature allows a farm administrator to give one site's administrators, special permission to manage the store. These rights are normally reserved for farm administrators.

Paths:

- **Default store path:** View, type, or browse for the physical path to the virtual disk folder that this store represents. The default path is used by all provisioning servers that do not have an override store path set.

  > **Note:**
  >
  > If you are setting an override store path in the **Server Properties** dialog, the path must be set before creating a version of the virtual disk. Because this path information is stored and referenced in the .vhdx header information, changing the path after versioning can cause unexpected results.

- **Default write cache paths:** View, add, edit, remove, or move the default write cache paths for this store. Entering more than one write cache path allows for virtual disk load to be distributed to physically different drives. When a target device first connects, the Stream Service picks from the list. The order of the write cache paths, for any override paths in the server store properties, must match the order of the write cache paths specified here.
- **Validate:** Click to validate store path selections from the **Validate Store Paths** dialog. The validation results display under the **Status** column.

Servers:

- **Site:** View or scroll to select the site where provisioning servers that can access this store exist. Multiple sites can access the same store.
- **Servers that provide this store:** All provisioning servers within the selected site display in this list. Check the box next to all servers that are permitted to access this store. If the store is only for a specific site, only those servers within that site are valid selections. If the default path is not valid for a selected provisioning server, you must define an override path in that server properties dialog, on the **Store** tab.
- **Validate:** Click to validate store path selections from the **Validate Store Paths** dialog. The validation results display under the **Status** column.

Device collections

Use device collections to create and manage logical groups of target devices. Creating device collections simplifies device management by performing actions at the collection level rather than at the target-device level.

> **Note:**
>
> A target device can only be a member of one device collection.

> A device collection might represent a physical location, a subnet range, or a logical grouping of target devices. A collection might consist of all target devices that use a particular virtual disk image, and that target device collection might consist of maintenance, test, and production devices. Alternatively, three device collections might exist for a particular virtual disk: one consisting of production devices, one consisting of test machines, and another consisting of maintenance machines. In the proceeding examples, devices in a given collection are assigned to the same disk.

Depending on a sites preference, another collection use case might include the consolidation of test or maintenance devices into a single device collection. Then manage virtual disk assignments on a per device basis rather than a per collection basis. For example, create a device collection labeled *Development* consisting of five target devices, each one assigned to a particular virtual disk.

Farm administrators create and manage device collections, or site administrators that have security privileges to that site. Collections are also created and managed by device administrators that have security privileges to that collection.

Expanding a device collection folder in the Citrix Provisioning™ console's tree allows you to view members of a device collection. To display or edit a device collection's properties, right-click on an existing device collection in the console, then select the **Properties** menu option. The **Device Collection Properties** dialog appears. Use this dialog to view or modify that collection. The IPv6 address is displayed if the target is configured to use IPv6.

> **Tip:**
>
> You can perform actions on members of a device collection, such as rebooting all target devices members in this collection.

Importing target devices into a collection

The **Import Target Devices Wizard** allows you to import the target device information from a file. Save the target device information as a `.csvfile`, then import it into a device collection.

> **Note:**
>
> The `.csv` text file can be created with a `.txt` file, NotePad.exe, or Excel. It contains one line per target device, which is formatted as:

```
DeviceName,MAC-Address,SiteName,CollectionName,Description,Type
```

Where:

`DeviceName = Name of new target device MAC-Address = MAC address of new device; such as 001122334455, 00-11-22-33-44-55, or 00:11:22:33:44:55 Type = 0 for production, 1 for test, or 2 for maintenance`

> Access the wizard from the farm, site, and device collection right-click menus. If it's accessed from the site or collection, only those target devices in the import file matching the site and collection by name are included in the import list.

The wizard also provides the option to automatically create the site or collection using the information in the file, if either does not exist. There is also the option to use the default collection's device template, if it exists for that collection.

A log file is generated with an audit trail of the import actions. For Windows Server 2008 R2, the file is located in:

`C:\\Documents and Settings\\All Users\\Application Data\\Citrix\\Provisioning Services\\log`

All other Windows Server operating systems generate the log file in `C:\ProgramData`.

To import target devices into a collection

1. In the console, right-click on the device collection, then click **Target Device>Import devices**. The **Import Target Devices Wizard** displays.
2. Type or browse for the file to import. The target device information is read from the file and displays in the table. Information can include the target device name, MAC address, and optionally description.
3. Highlight one or more target devices to import. If applying the collection template to the imported target devices, select the **Apply collection template device** when creating devices check box.
4. Click **Import** to import the .csv text file containing target device information, into the selected collection. The status column indicates if the import was successful.

Refreshing a collection in the Citrix Provisioning console

After changing a collection, refresh the collection before those changes appear in the console. To refresh, right-click on the collection in the tree, then select the **Refresh** menu option.

Booting target devices within a collection

To boot target devices within a collection:

1. Right-click on the collection in the console, then select the **Target Device>Boot** menu option. The **Target Device Control** dialog displays with the **Boot devices** menu option selected in the **Settings** menu. Target devices display in the **Device** table.

2. Click the **Boot** devices button to boot target devices. The **Status** column displays the **Boot Signal** status until the target device successfully receives the signal, then status changes to *Success*.

Restarting target devices within a collection

To restart target devices within a collection:

1. Right-click on the collection in the console tree, then select the **Target Device>Restart** devices menu option. The **Target Device Control** dialog displays with the **Restart devices** menu option selected in the **Settings** menu. Devices display in the **Device** table.
2. Type the number of seconds to wait before restarting target devices in the **Delay** text box.
3. Type a message to display on target devices in the **Message** text box.
4. Click the **Restart devices** button to restart target devices. The **Status** column displays the restart signal status until the target device successfully receives the signal, then status changes to *Success*.

Shutting down target devices within a collection

To shut down target devices members within a collection:

1. Right-click on the collection in the console, then select the **Target Device>Shutdown** devices menu option. The **Target Device Control** dialog displays with the **Shutdown devices** menu option selected in the **Settings** menu. Target devices display in the **Device** table.
2. Type the number of seconds to wait before shutting down target devices in the **Delay** text box. Type a message to display on target devices in the **Message** text box.
3. Click the **Shutdown devices** button to shut down target devices. The **Status** column displays the shutdown signal status until the target device shuts down. As each target device successfully shuts down, the status changes to *Success*.

Sending messages to target devices within a collection

To send a message to target device members within a collection:

1. Right-click on the collection in the console tree, then select the **Target Device>Send message** menu option. The **Target Device Control** dialog displays with the **Message to devices** menu option selected in the **Settings** menu. Target devices display in the **Device** table.
2. Type a message to display on target devices in the **Message** text box.

3. Click the **Send message** button. The **Status** column displays the message signal status until the target device successfully receives the message, then the status changes to *Success*.

Moving collections within a site

Target devices can be moved from one collection to another collection within the same site.

To move a collection

1. In the console, expand the collection, right-click on the target device, then select the **Move** menu option.
2. From the menu, select the collection to move this target device into, then click **OK** to close the dialog.

Target devices

A device, such as desktop computer or server, that boots and gets software from a virtual disk on the network is considered a target device. A device that is used to create the virtual disk image is a considered a *master target device*.

The lifecycle of a target device includes:

- Preparing
  - A Master target device used for creating a virtual disk image
  - A target device that boots from a virtual disk image
- Adding target devices to a collection in the farm
  - From the Console
  - Using Auto-Add
  - Importing
- Assigning the target device type
- Maintaining target devices in the farm

After a target device is created, the device must be configured to boot from the network. Also, a virtual disk must be assigned to the device, and the set of Citrix Provisioning™ Servers to contact at boot time must be configured.

There are several types of target devices within a farm. For example, while a device is being used to create a virtual disk image, it is considered a Master target device. All other devices are configured as a particular device type. The device Type determines a devices current purpose, and determines if that device can access a particular virtual disk version that is in production, test, or maintenance.

The device Type is selected on the **General** tab of the **Target Device Properties** dialog, which includes the following options:

- Production: Select this option to allow this target device to stream an assigned virtual disk that is currently in production, the default.
- Maintenance: Select this option to use this target device as a maintenance device. Only a maintenance device can access and alter a virtual disk version that is in maintenance mode. Only the first maintenance device to boot the version while in maintenance mode is allowed to access that version.
- Test: Select this option to use this target device to access and test differencing disk versions that are currently in test mode.

A target device becomes a member of a device collection when it is added to the farm. The use of device collections simplifies the management of all target devices within that collection. A target device can only be a member in one device collection. However, a target device can exist in any number of views. If a target device is removed from the device collection, it is automatically removed from any associated views.

When target devices are added to a collection, that devices properties are stored in the Citrix Provisioning database. Target device properties include information such as the device name and description, boot method, and virtual disk assignments (see **Target device** properties for details).

Target devices are managed and monitored using the **Console and Virtual Disk Status Tray** utilities.

In the Citrix Provisioning console, actions can be performed on:

- An individual target device
- All target devices within a collection
- All target devices within a view

Target device properties

When configuring a target device, consider the following:

- A reboot is required if a target device is active when modifications are made to any of the following device properties: Boot from, MAC, Port, vDisks for this device.
- BitLocker encryption is not supported on a provisioned target device virtual disk.

The following tables define the properties associated with a target device.

General tab

FIELD	DESCRIPTION
Name	The name of the target device or the name of the person who uses the target device. The name can be up to 15 bytes in length. However, the target device name cannot be the same as the machine name being imaged. **Note:** If the target device is a domain member, use the same name as in the Windows domain. Use the same name unless that name is the same as the machine name being imaged. When the target device boots from the virtual disk, the name entered here becomes the target device machine name.
Description	Provides a description to associate with this target device.
Type	Select the access type for this target device from the menu, which includes the following options: **Maintenance** - Select this option to use this target device as a maintenance device which applies updates to a new maintenance version of a virtual disk. A maintenance device has exclusive read-write access to a maintenance version. **Test** - Select this option to use this target device to access versions that are in test mode. Test devices have shared read-only access to the test versions of a virtual disk to facilitate QA testing of a virtual disk version in standard image mode. Perform this task before releasing that version to production machines. **Production** - Select this option to allow the target device to stream an assigned virtual disk that is currently in

FIELD	DESCRIPTION
	production. Production devices have shared, read-only access to production versions of a virtual disk. Production devices do not have access to maintenance or test versions. This prevents untested updates from accidentally being deployed on production machines. **Note:** The default Type for a new device is maintenance. The default type for an existing device is maintenance.
Boot from	The boot method used by this target device. Options include booting from a virtual disk, hard disk, or floppy disk.
MAC	Enter the media access control (MAC) address of the NIC that is installed in the target device.
Port	Displays the UDP port value. In most instances, you do not have to change this value. However, if target device software conflicts with any other IP/UDP software, that is, they are sharing port, you must change this value.
Class	Class used for matching new vDisks to target devices when using automatic disk image update to match new vDisks images to the appropriate target devices.
Disable this device	Enable this option to prevent target devices from booting. Regardless if enabled or disabled, new target devices that are added using Auto-add, have records created in the database.

vDisks tab

FIELD	DESCRIPTION
vDisks for this device	Displays the list of virtual disk assigned to this target device, including the following options:

FIELD	DESCRIPTION
	Click **Add** to open the **Assign vDisks** dialog. To filter the displayed vDisks, select a specific store name and Provisioning Server or select **All Stores and All Servers**. This process lists all vDisks available to this target device. Highlight the vDisks to assign, then click **OK**. Click **Remove** to remove vDisks from this device. Click **Printers** to open the **Target Devices vDisk Printers** dialog. This dialog allows you to choose the default printer and any network and local printers to enable or disable for this target device.

Personality tab

FIELD	DESCRIPTION
Options	Provides secondary boot options: Include the local hard drive as a boot device; Include one or more custom bootstraps as boot options. If enabling a custom bootstrap, click **Add**, to enter the bootstrap file name and the menu text to appear (optional), then click **OK**. If more than one virtual disk is listed in the table or if either (or both) secondary boot options are enabled, you are prompted with a disk menu when it is booted. Enter a menu option name to display to the target device. The target device can select which boot options to use. Click **Edit** to edit an existing custom bootstrap's file name or menu text. Click **Remove** to remove a custom bootstrap file.
Name and string	There are no fixed limit to the number of names you can add. However, the maximum name length is 250 characters and the maximum value length is 1000 characters. Use any name for the field **Name**, but do not repeat a field name in the same target device. Field names are not case sensitive. In other words, the system interprets *FIELDNAME* and

FIELD	DESCRIPTION
	fieldname as the same name. Blank spaces entered before or after the field name are automatically removed. A personality name cannot start with a $. This symbol is used for reserved values such as $DiskName and $WriteCacheType.

Status tab

FIELD	DESCRIPTION
Target device status	The following target device status information appears: **Status** - current status of this device (active or inactive); **IP Address** - provides the IP Address or 'unknown'; **Server** - the provisioning server that is communicating with this device; **Retries** - the number of retries to permit when connecting to this device; **vDisk** - provides the name of the vDisk or displays as 'unknown'; **vDisk version** - version of this vDisk currently being accessed; **vDisk full name** - the full file name for the version currently being accessed; **vDisk access** - identifies if the version is in production, maintenance, or test; **License information** - depending on the device vendor, displays product licensing information including; n/a, Desktop License, Datacenter License, or Citrix Virtual Apps and Desktops License.

Note:

If a target uses IPv6, then its IPv6 address is displayed.

Logging tab

FIELD	DESCRIPTION
Logging level	Select the logging level or select **Off** to disable logging: **Off** – Logging is disabled for this provisioning server. **Fatal** – logs information about an operation that the system might not recover from. Error log information about an operation that produces an error condition; **Warning** – logs information about an operation that completes successfully, but there are issues with the operation; **Info** – Default logging level. Logs information about workflow, which generally explains how operations occur. **Debug** – logs details related to a specific operation and is the highest level of logging. If logging is set to DEBUG, all other levels of logging information are displayed in the log file. **Trace** – logs all valid operations.

Setting the target device as the template for this collection

A target device can be set as the template for new target devices that are added to a collection. A new target device inherits the properties from the template target device, which allows you to quickly add new devices to a collection.

> **Tip**

> Target devices using virtual disks are created and added to a collection when running the Citrix Virtual Apps and Desktops™ Setup Wizard. If a target device template exists, it is ignored when the target device using a virtual disk is added to the collection.

> To set a target device as the template device for a collection, in the console, right-click on the target device, then select the **Set device as template** option.

Consider the following when using templates:

- Disable the target device that serves as the template. Disabling it adds all target devices using this template to the database, but does not permit the target device to boot.

- Target devices receive a message requesting that they first contact the administrator before being allowed to boot.
- *T* appears in light blue on the device serving as the template. New target devices automatically have a name generated and all other properties are taken from the default template target device. No user interaction is required.

Creating a VM with nested virtualization

Sometimes, you want to create a nested virtualization paradigm for a VM. If your environment uses Device Guard and you want to create a template from the VM running it, consider that Citrix Provisioning is unaware that it was set up for that particular VM. To resolve this issue, manually enable Device Guard on the Hyper-V host using a PowerShell command. Perform this operation after the VM has been created using the Citrix Virtual Apps™ and Desktops Setup Wizard.

To configure a VM to use Device Guard:

1. Create the VM using the Citrix Virtual Apps and Desktops Setup Wizard.
2. After creating the VM, run the following command for each VM on the physical Hyper-V host to enable nested virtualization:

   ```
   Set-VMProcessor -VMName <Target VM's Name> -ExposeVirtualizationExtensions $true
   ```

> **Tip:**
>
> See the Microsoft site for more information about nested virtualization.

Copying and pasting target device properties

To copy the properties of one target device, and paste those properties to other target device members:

> **Note:** Target devices that use virtual disks can only inherit the properties of another target device that uses one.

1. In the Citrix Provisioning console's **Details** pane, right-click on the target device that you want to copy properties from, then select **Copy device properties**. The **Copy Device Properties** dialog appears.

2. Select the check box next to the properties that you want to copy, then click **Copy**. The properties are copied to the clipboard and the dialog closes.
3. Right-click on one or more target devices that inherit the copied properties, then select the **Paste** menu option. The **Paste Device Properties** dialog appears.
4. Click **Close** to close the dialog.

Booting target devices

1. Right-click on a collection to boot all target devices in the collection. Or, highlight only those target devices that you want to boot within the collection tree, then select the **Boot devices** menu option. The **Target Device Control** dialog displays with the Boot devices menu option selected in the **Settings** menu.
2. Click the Boot devices button to boot target devices. The **Status** column displays the **Boot Signal** status until the target device successfully receives the signal, then status changes to Success.

Checking a target device's status from the console

The target device status indicates whether it is active or inactive on the network.

To check the status of a target device:

1. Double-click on the target device in the console window, then select the **Properties** menu option. The **Device Properties** tab appears.
2. Select the **Status** tab and review the following status information:
    - Status, active, or inactive
    - IP address
    - Current provisioning server
    - Current virtual disk name
    - Provisioning server cache file size in bytes If the target device is active in the console window, the target device icon appears as a green computer screen. If the target device is inactive, the icon appears as a black computer screen.

Sending messages to target devices

To send a message to target devices members:

1. Right-click on the collection to send a message to all members within the collection. Or, highlight only those target devices within the collection that receive the message, then select the **Send** message menu option. The **Target Device Control** dialog displays with the Message to devices menu option selected in the **Settings** menu. Target devices are displayed in the **Device** table.
2. Type a message to display on target devices in the **Message** text box.
3. Click the Send message button. The **Status** column displays the **Message Signal status** until target devices successfully receives the message, the status changes to **Success**.

Shutting down target devices

To shut down target devices:

1. Right-click on the collection to shut down all target devices within the collection. Or, highlight only those target devices to shut down within a collection, then select the **Shutdown devices** menu option. The **Target Device Control** dialog displays with the Shutdown devices menu option selected in the **Settings** menu. Target devices display in the Device table.
2. Type the number of seconds to wait before shutting down target devices in the **Delay** text box.
3. Type a message to display on target devices in the **Message** text box.
4. Click the **Shutdown devices** button to shut down target devices. The **Status** column displays the shutdown signal status until the target device shuts down. As each target device successfully shuts down, the status changes to **Success**.

Restarting target devices

To restart target devices:

1. Right-click on a collection in the console tree or highlight only those target devices you want to restart within the collection. Select the **Restart devices** menu option. The **Target Device Control** dialog displays with the **Restart devices** menu option selected in the **Settings** menu. Target devices display in the **Device** table.
2. Type the number of seconds to wait before restarting target devices in the **Delay** text box.
3. Type a message to display on target devices in the **Message** text box.
4. Click the **Restart devices** button to restart target devices. The **Status** column displays the **Restart Signal** status until the target device successfully receives the signal, then status changes to **Success**.

Moving target devices between collections

A target device can be moved from one collection to another collection within a site by dragging it into the console's **Details** pane. Drag the device from one collection, then drop the device into another collection. Alternatively, target devices can be moved using the **Move** menu option.

To move a target device using the **Move** menu option:

1. In the console, expand the collection, right-click on the target device in the **Details** pane, then select the **Move** menu option.
2. From the menu, select the collection to move this target device into. If necessary, apply the collection's device template to the target device being moved by enabling the option **Apply target collection's template device properties**.
3. Click **Move**.

> **Tip:**

> There is a risk that moving target devices from site to site can cause them to be deleted in the future. This risk increases if the target device was created using the Streamed VM Setup Wizard. You can use the interface to move target devices from one site to another site, however, Citrix® recommends that you avoid moving them from site to site using this method.

Managing target device personality

Normally, all target device's sharing virtual disk must have identical configurations. The **Target Device Personality** feature allows you to define data for specific target devices and make it available to the target device at boot time. This data is used by your custom applications and scripts for various purposes.

The number of fields and amount of data that you can define for each target device is limited to 64 Kb or 65,536 bytes per target device. Each individual field contains up to 2,047 bytes.

Target device personality tasks

- Define personality data for a single target device using the console
- Define personality data for multiple target devices using the console
- Using target device personality data

Define personality data from a single target device using the console

To define personality data for a single target device:

1. In the Console, right-click on the target device that you want to define personality data for, then select the **Properties** menu option.
2. Select the **Personality** tab.
3. Click the **Add** button. The **Add/Edit Personality String** dialog appears. **Note:** There is no fixed limit to the number of field names and associated strings you can add. However, the total amount of personality data assigned to a single string, names, and data, combined, is approximately 2,047 bytes. Also, the total amount of data contained in names, strings and delimiters is limited to approximately 64 Kb or 65,536 bytes per target device. This limit is checked when you attempt to add a string. If you exceed the limit, a warning message displays and you are prevented from creating an invalid configuration. Target device personality data is treated like all other properties.
4. Enter a name and string value.

> **Note:**
>
> You can use any name for the field. **Name**, but you cannot repeat a field name in the same target device. Field names are not case sensitive. In other words, the system interprets *FIELDNAME* and *fieldname* as the same name. Blank spaces entered before or after the field name are automatically removed. A personality name cannot start with a $. This symbol is used for reserved values such as $DiskName and $WriteCacheType.

5. Click **OK**.

To add more fields and values, repeat Steps 5 and 6 as needed. When finished adding data, click **OK** to exit the **Target Device Properties** dialog.

Define personality data for multiple target devices using the console

Define target device personality for multiple devices:

1. In the console, right-click on the target device that has the personality settings that you want to share with other device, then select **Copy**. The **Copy device properties** dialog appears.
2. Highlight the target devices in the **Details** pane that you want to copy personality settings. Right-click and select the **Paste device properties** menu.

3. Click the **Personality strings** option, or, alternately choose to copy other properties. Click **Paste**.

Using target device personality data

Once the file system becomes available to the target device, the personality data is written to a standard Windows .ini text file called *Personality.ini*. The file is stored in the root directory of the virtual disk file system, your custom scripts or applications access this file.

The file is formatted as follows:

```
`[StringData]

FieldName1=Field data for first field

FieldName2=Field data for second field`
```

This file is accessible to any custom script or application and is queried by the standard Windows .INI API. Also, a command line application, called `GetPersonality.exe`, permits easier batch file access to the personality settings.

A target device's virtual disk name and mode can be retrieved using GetPersonality.exe. The following reserve values are included in the section of the Personality.ini file:

```
$DiskName=&lt;xx>

$WriteCacheType=<0 (Private image)

All other values are standard image; 1 (Server Disk), 2 (Server Disk
Encrypted), 3 (RAM), 4 (Hard Disk), 5 (Hard Disk Encrypted), 6 (RAM Disk),
or 7 (Difference Disk). Min=0, Max=7, Default=0>
```

The xx field is the name of the disk. A virtual disk name cannot start with a $. This symbol is used for reserved values such as $DiskName and $WriteCacheType. The following message displays if a name that starts with $ is entered:

`A name cannot start with a $. This is used for reserve values like $DiskName and $WriteCacheType. The $DiskName and $WriteCacheType values can be retrieved on the target device using GetPersonality.exe.`

GetPersonality.exe

The command line utility **GetPersonality.exe** allows users to access the **Target Device Personality** settings from a Windows batch file. The program queries the INI file for the user and places the personality strings in the locations chosen by the user. GetPersonality.exe supports the following command line options:

```
`GetPersonality FieldName /r=RegistryKeyPath <- Place field in registry

GetPersonality FieldName /f=FileName <- Place field in file

GetPersonality FieldName /o <- Output field to STDOUT

GetPersonality /? or /help <- Display help`
```

Setting environment variables

Setting environment variables with personality data is a two-step process:

1. Use the **GetPersonality** command with the /f option to insert the variable into a temporary file.
2. Use the set command to set the variable. For example, to set the environment variable Path statement for the target device a personality name, define the Pathname with the string value:

   ```
   `%SystemRoot%;%SystemRoot%\System32\Wbem;C:\Program Files\Microsoft Office\OFFICE11\;C:\Program Files\Microsoft SQL Server\80\Tolls\Binn`
   ```

   The `/f` option creates a temporary file, allowing for a name to be assigned, in this case `temp.txt`. The following lines are included in the batch file:

   ```
   `GetPersonality Pathname /f=temp.txt

   set /p Path= <temp.txt`
   ```

   Note:

   If the file name specified with the `/f` option exists, *Get Personality* does not append the line to the file. Instead, the existing line is overwritten in the file.

Changing the device status to down

Occasionally, a target device displays as active when it is down. This situation occurs when the status record is not refreshed properly in the database. To change the target device's status in the database to down, Complete the following steps:

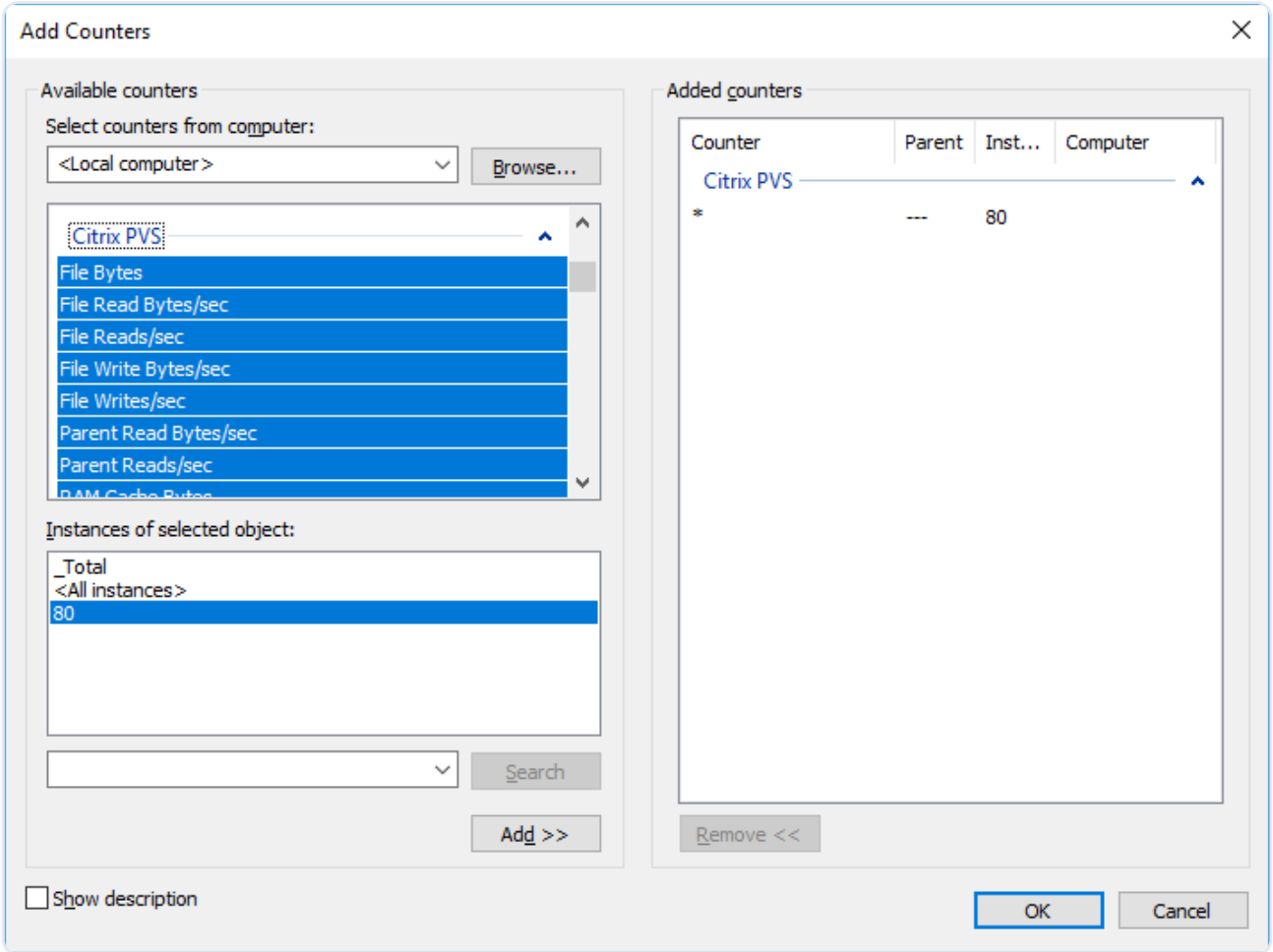
1. In the console, right-click on the target device marked as down, then select the **Mark Device Down** option. A confirmation dialog appears.
2. Click **OK** to mark the device as down.

Support for windows performance counters

Citrix Provisioning target devices provide Windows performance counters for each storage tier:

- RAM cache
- VHDX file
- network streaming

Using these performance counters, you can monitor target device streaming IOPS, bandwidth usage, current RAM usage, and VHDX file size.



Boot Device Management support for UEFI using the Citrix Virtual Apps and Desktops Setup wizard

UEFI BDM integrates with the Citrix Virtual Apps and Desktops Setup wizard, which allows you to set the BDM boot option to target UEFI firmware. With this support, Citrix Provisioning supports booting from:

- ISO
- USB
- Boot partitions

Consider the following:

- BDM support for UEFI can only be used by VMs that have a BDM disk.
- This functionality uses Citrix Provisioning Server information provided by you that function as login servers for the UEFI target VMs.

> **Tip:**
>
> During UEFI boot, detailed information about the server and vDisk is displayed on the console of the booting machine.

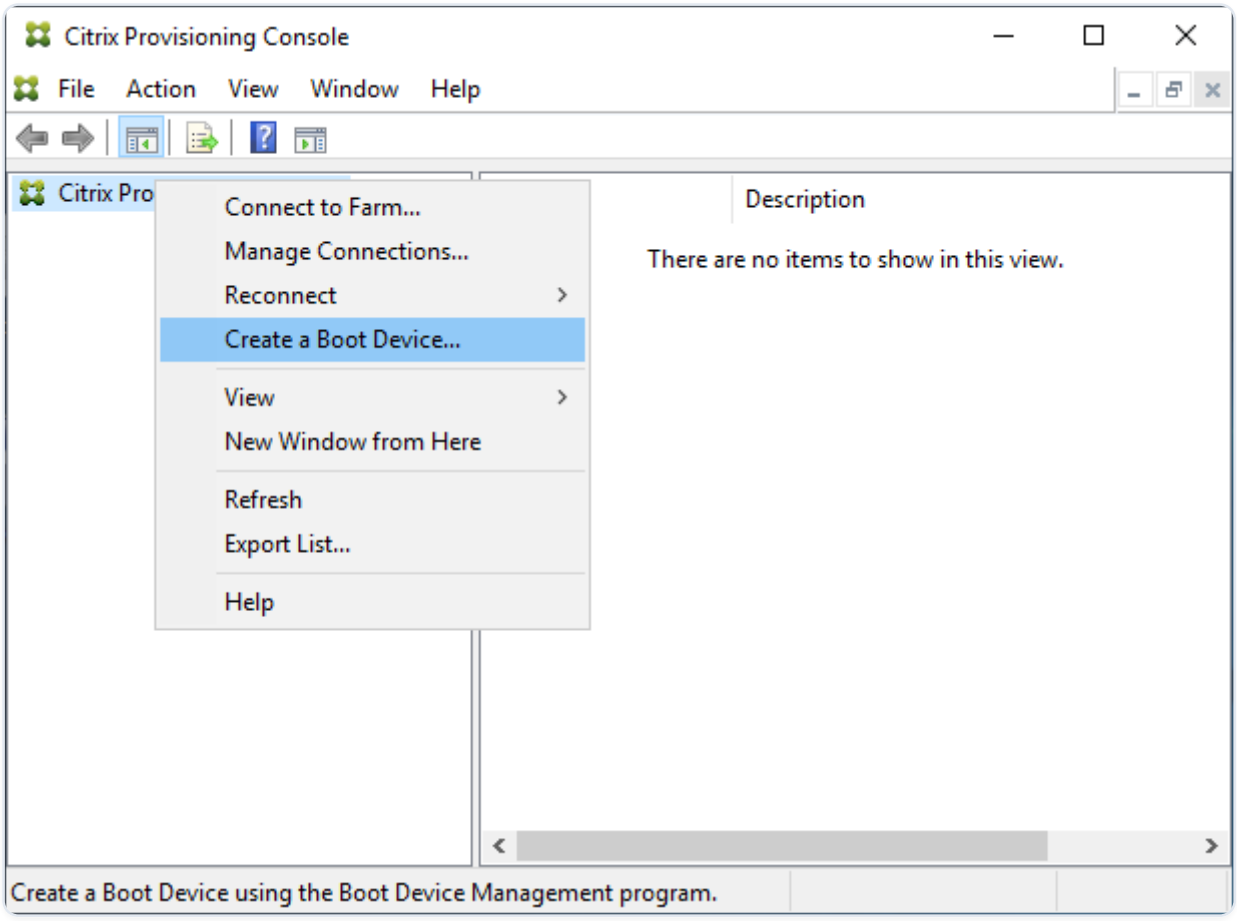
Setting a target device for UEFI firmware

To create target VMs using BDM boot, use one of the following ways:

- Use the Citrix Virtual Apps and Desktops Setup Wizard, and select BDM as the boot mode. For more information, see Run the wizard.
- If you want to manually create VMs, you can create a BDM boot disk VDH file using the **Create a Boot Device** option. To do this:

  a. Select the Citrix Provisioning Console node and right-click to display a context menu.

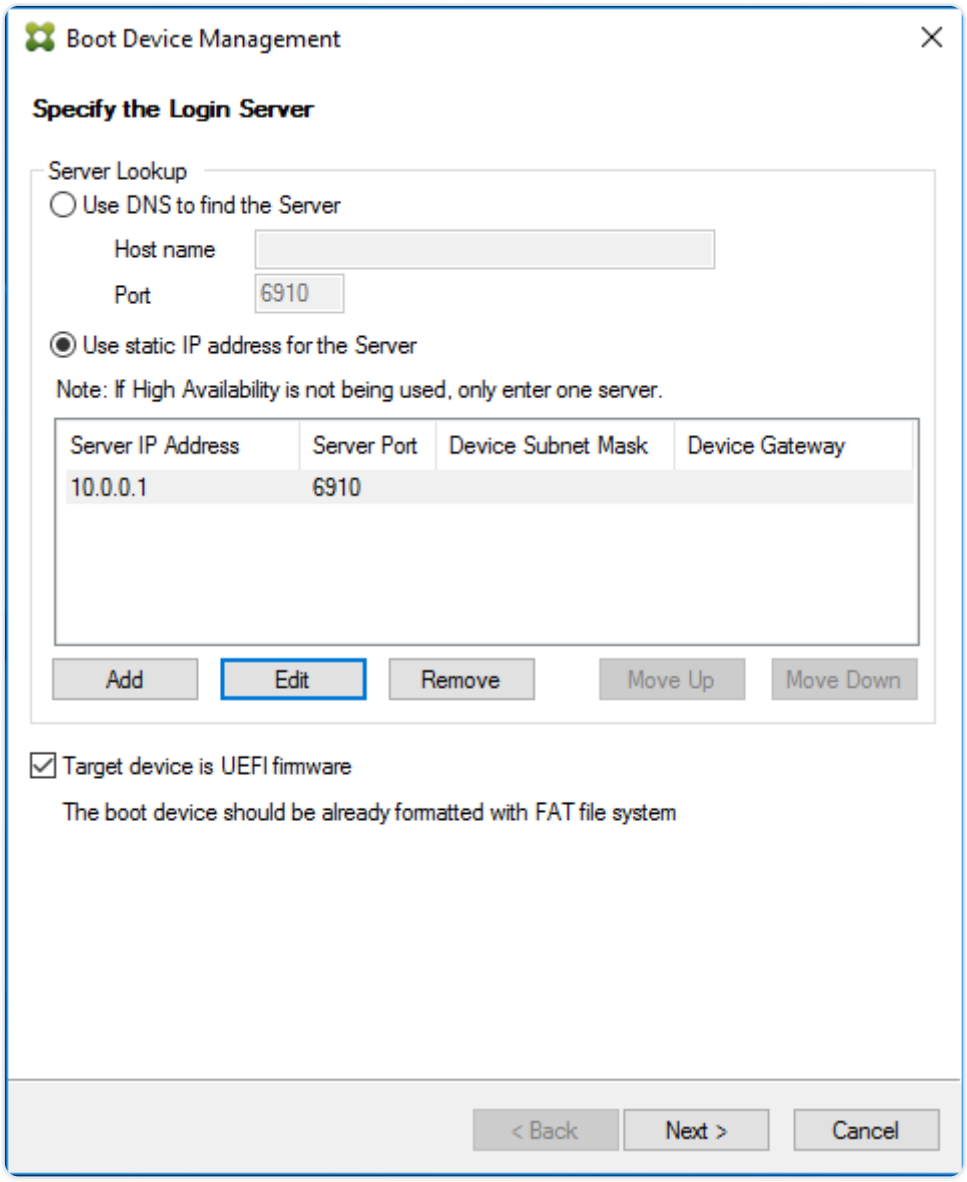
  b. In the context menu, select **Create a Boot Device**.



On the **Boot Device Management** screen:

1. Select **Target device is UEFI firmware**.
2. Click **Next**.

You can also access the **Boot Device Management** screen from the **Start** menu. See Server lookup using DHCP to retrieve the device IP address for more information.



Tip:

You can update the BDM partition with server information using the Boot Device Management screen.

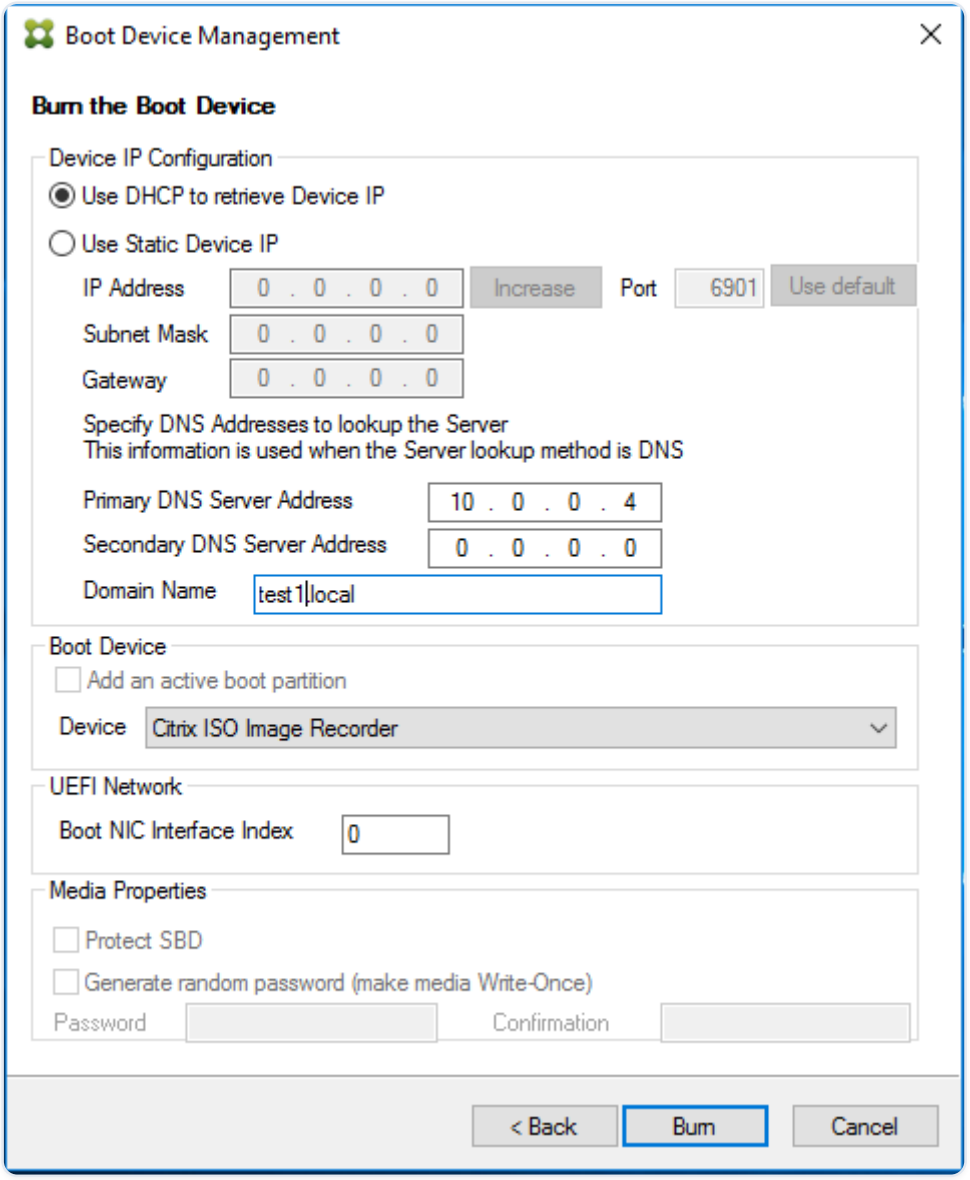
Server look up using DHCP to retrieve the device IP address

When specifying a login server, you have the option to use either DNS to locate a server, or you can specify a static IP address to identify a server. If the server lookup method is set to **Use DNS to find a Server**, you can set extra UEFI options, including:

- UEFI network. Use this option to set the boot NIC interface index value. By default, this value is set to 0. This value represents the first NIC.

- Boot Device. Select the **Add an active boot partition** check box, and use the drop-down menu to select from the following device options:
  - Citrix ISO Image Recorder. This is the default choice for UEFI networks.
  - USB. Use this device option if a USB drive is connected to the Provisioning server.
  - HDD. When the boot device is a directly connected hard disk drive.

After specifying BDM configuration options, click **Burn** to create a BDM device.



Important:

Citrix recommends that you do not use HDD as a boot option when connected to the Provisioning server.

Updating a BDM partition

You can update the BDM boot disk of target VMs:

- created using the Citrix Virtual Apps and Desktops Setup Wizard, and
- in a collection, a group of selected target VMs, or an individual target VM.

> **Note:**
>
> Provisioned devices must be turned off when updating a BDM boot partition.

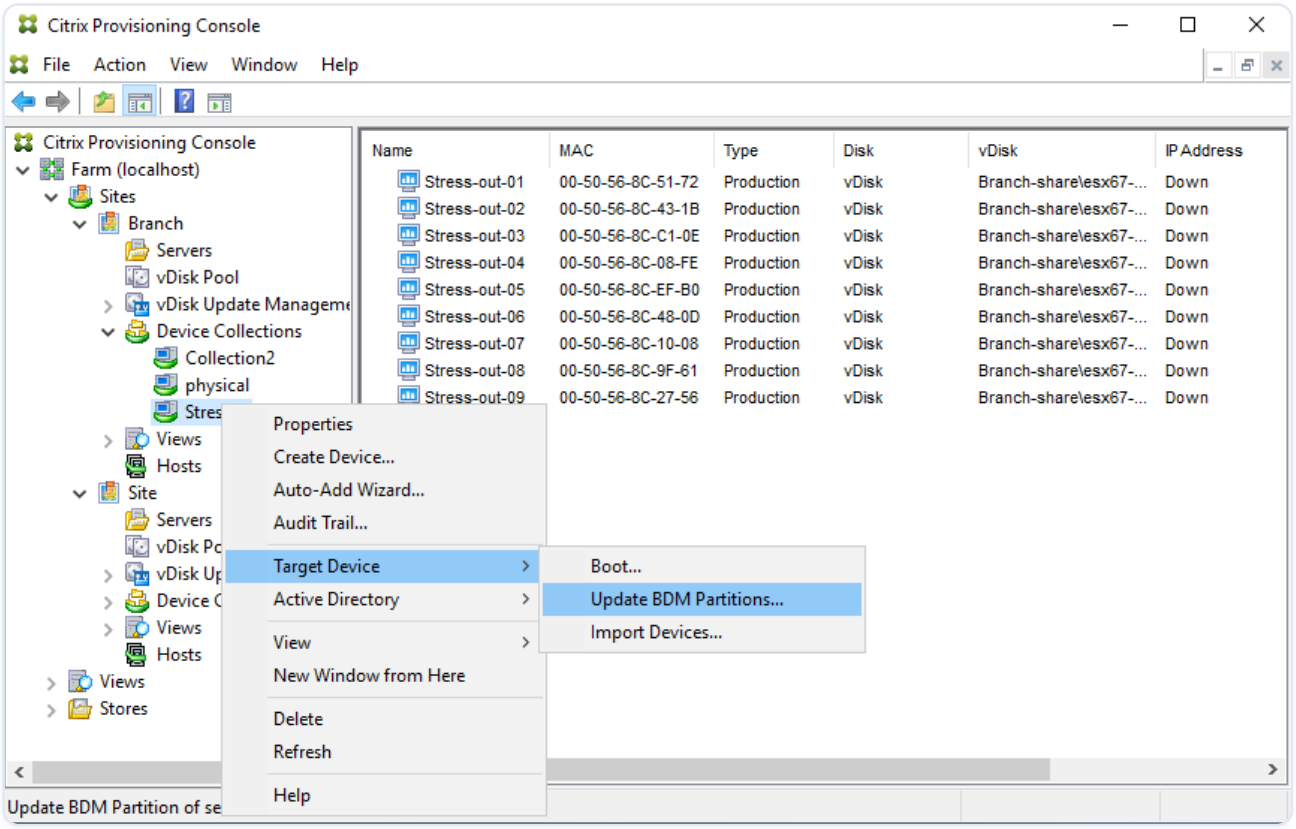
> The BDM boot partition upgrade does not require PXE, TFTP, or TSB. At boot time it automatically loads all relevant Provisioning server information from the BDM disk and does not need external services provided by PXE and TFTP.

Update BDM boot disks

To update the BDM boot disks, do the following:

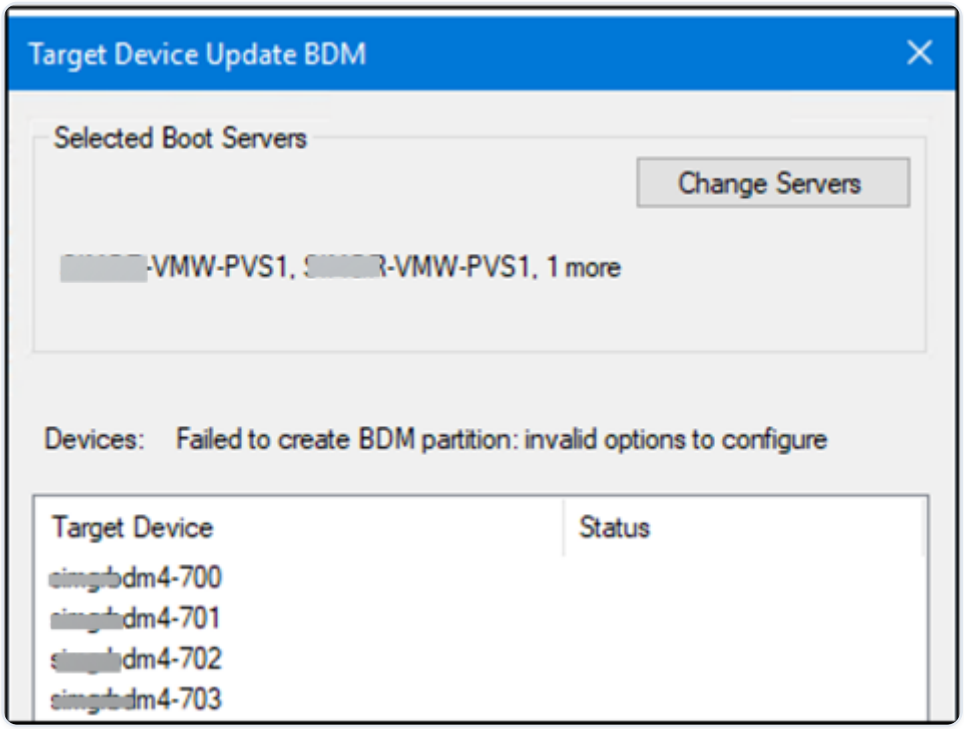
> **Note:**
>
> You cannot do a BDM update using the Citrix Provisioning Console if you install Citrix Provisioning Servers on the system running Windows Server Core.

1. In the Citrix Provisioning Console, expand **Device Collections**, and and select either a collection or a group of targets within a collection or a single target.
2. Right-click to expose a context menu.
3. In the context menu, select **Target Device**, then select **Update BDM Partitions**.



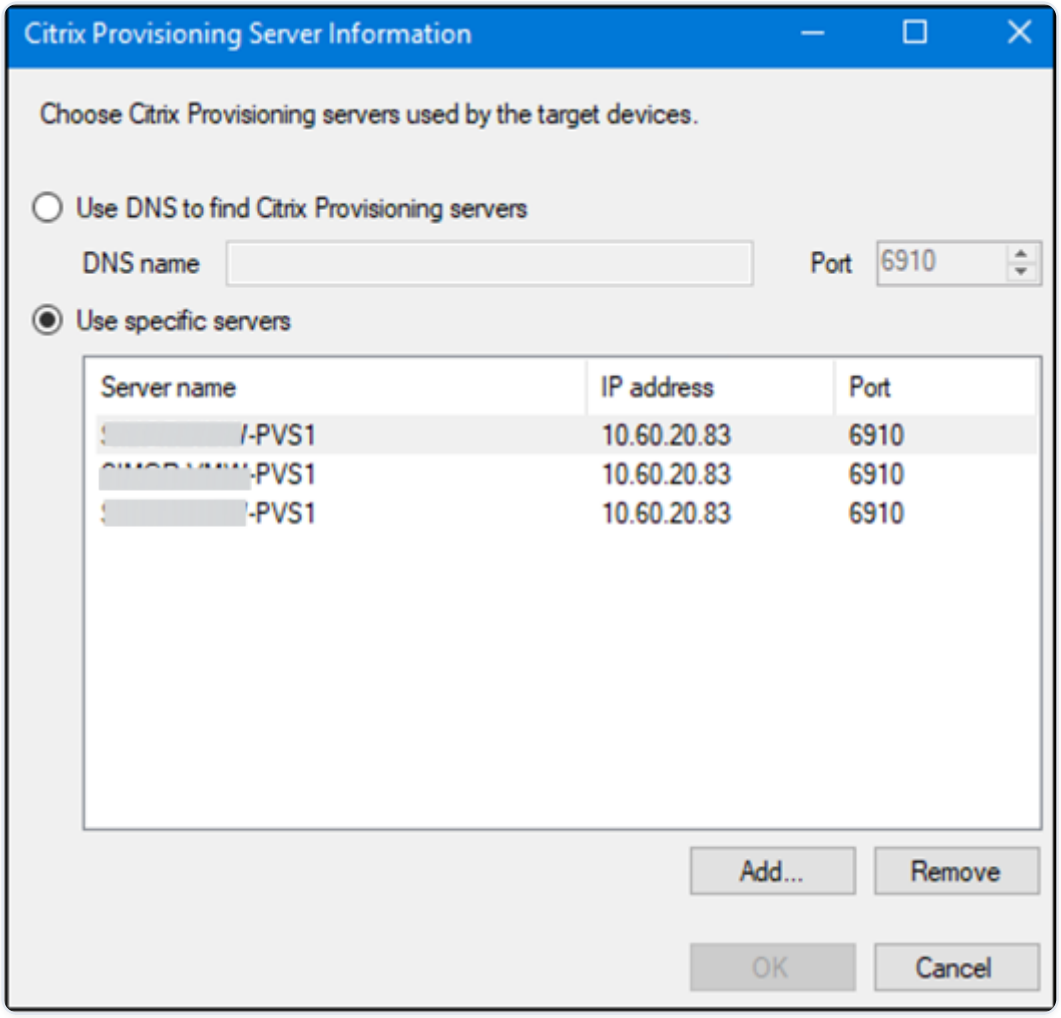
On the **Target Device Update BDM** screen:

1. Click **Change Servers**.



2. On the **Citrix Provisioning Server Information** dialog, the current set of servers are displayed. You can update the list. You can add individual servers using the **Add** button, or use

a single DNS name that translates to the set of IP addresses used by the servers to connect to at the boot time.



3. Click **OK** to return to the **Target Device Update BDM** page.
4. Click **Update Devices**. Once selected, Citrix Provisioning begins updating all target devices with the BDM update.
5. Click **Stop** to immediately halt the update process.
6. Click **Close** to dismiss the Target Device Update BDM screen. The process continues to run in the background.

Note:

You can currently specify a maximum of 4 login servers at this time.

vDisks

vDisks are managed throughout their lifecycle. Full image lifecycle takes a vDisk from creation, through deployment and subsequent updates, and finally to retirement. The lifecycle of a vDisk consists of four stages:

1. Creating
2. Deploying
3. Updating
4. Retiring

When provisioning target devices, consider the following:

- To have a single vDisk, all target devices must have certain similarities to ensure that the OS has necessary drivers required to run properly. The three key components are the motherboard, network card, or video card.
- Install and configure OEM NIC teaming software before you install the target device software.
- Identify target devices by the operating system running on the device.
- Dual boot vDisk images are not supported.
- BitLocker encryption is not supported on a provisioned target device vDisk.

See System requirements for more information.

Creating a vDisk

Creating a vDisk includes:

- preparing the master target device for imaging
- creating and configuring a vDisk file where the vDisk resides
- imaging the master target device to that file

These steps result in a new base vDisk image. This process can be performed automatically, using the Imaging Wizard, or manually. You can also create a common image for use with a single target platform or for use with multiple targets. For details, see Creating vDisks.

Deploying a vDisk

After a vDisk base image is created, it is deployed by assigning it to one or more devices. A device can have multiple vDisk assignments. When the device starts, it boots from an assigned vDisk. There are two boot mode options; Private Image mode (single device access, read/write), and

standard image mode (multiple devices, write cache options). For more details, see *Prerequisites for deploying vDisks* later in this article.

Updating a vDisk

It is often necessary to update an existing vDisk so that the image contains the most current software and patches. Updates can be made manually, or the update process can be automated using vDisk Update Management features. Each time a vDisk is updated a new version is created. Different devices can access different versions based on the type of target device and version classification. A maintenance device can have exclusive read/write access to the newest maintenance version. Test devices can have shared read-only access to versions classified as test versions. Production devices can have shared read-only access to production versions. Versions are created and managed from the **vDisk Versioning Dialog**. An update can also be the result of merging versions. For more details on updating vDisks, see Updating vDisks.

Retiring a vDisk

Retiring a vDisk is the same as deleting. The entire VHDX chain including differencing and base image files, properties files, and lock files, are deleted. For details, see Retiring or deleting virtual disks.

> **Note:**
>
> In addition to those vDisk tasks performed within a disk's lifecycle, there are also other vDisk maintenance tasks that can be performed. These include importing or exporting the vDisk, backing-up vDisks, replicating, and load balancing.

Prerequisites for deploying vDisks

vDisks are configured before being deployed. Configuration tasks include:

- Selecting the vDisk access mode and if applicable, the write cache mode. See Selecting the write cache destination for standard vDisk images.
- Configuring the vDisk for Microsoft Volume Licensing. For details, see Configuring a vDisk for Microsoft Volume Licensing.
- Enabling Active Directory machine account password management, if applicable.

Selecting the write cache destination for standard vDisk images

Citrix Provisioning™ supports several write cache destination options. The write cache destination for a vDisk is selected on the **General** tab, which is available from the vDisk File Properties dialog.

Considerations and requirements

- Consider the impact of using the server-side persistent write cache. Persistent cache is only used where unauthorized users have access to a machine. Ensure that machines are not shared among users.
- When selecting cache on local hard drive, ensure that the hard-disk drive is formatted with NTFS for Window devices, with a minimum of 500 MB.
- When selecting cache on the target device RAM and standard image mode, the registry setting WcMaxRamCacheMB (a DWORD) in the BNIStack Parameters determines the max size of the RAM write cache. If the registry entry does not exist, then the default value used is 3584 MB.
- Citrix Provisioning version 7.7 only supports the use of Microsoft System Center Configuration Manager (ConfigMgr) Client as follows:

CONFIGMGR CLIENT	CACHE ON DEVICE HARD DRIVE	CACHE IN DEVICE RAM WITH OVERFLOW ON HARD DISK	CACHE IN DEVICE RAM
ConfigMgr 2012	**Supported**	**Supported**	Not supported
ConfigMgr 2012 SP1	**Supported**	**Supported**	Not supported
ConfigMgr 2012 R2	**Supported**	**Supported**	Not supported

CONFIGMGR CLIENT	CACHE ON SERVER	CACHE ON SERVER PERSISTED	CACHE ON DEVICE HARD DRIVE PERSISTED
ConfigMgr 2012	Not supported	Not supported	Not supported
ConfigMgr 2012 SP1	Not supported	Not supported	Not supported
ConfigMgr 2012 R2	Not supported	Not supported	Not supported

The following sections describe all valid write cache destination options.

Note:

Provisioning Services version 7.12 introduced Linux streaming. When using this feature, consider that caching options on a Linux target device are the same on a Windows device. For more information about Linux streaming, see Installation.

Cache on device hard drive

Write cache can exist as a file in NTFS format, or on the target-device's hard drive. This option frees up the server. It does not process write requests because it does not have the finite limitation of RAM.

The hard drive does not require any additional software to enable this feature.

Note:

The write cache file is temporary unless the vDisk mode is set to **Private Image mode**.

Important:

The vDisk cache type field **Cache on device hard drive** is deprecated and will be removed in a future release. Citrix recommends using one of the other available cache types. For more information, see the Deprecation article.

Cache on device hard drive persisted (experimental phase only)

The same as Cache on device hard drive, except cache persists. This write cache method is an experimental feature and is supported only for NT6.1 or later. This method also requires a different bootstrap. To click the correct bootstrap from the console, right-click on the provisioning server, select **Configure Bootstrap**. On the **General** tab, click the **Bootstrap** file option, then choose **CTXBP.BIN**. Citrix recommends that the local HDD (client side) drive has enough free space to store the entire vDisk.

Important:

> The vDisk cache type field **Cache on hard drive persisted** is deprecated and will be removed in a future release. Citrix recommends using one of the other available cache types. For more information, see the Deprecation article.

Cache in device RAM

Write cache can exist as a temporary file in the target device's RAM. It provides the fastest method of disk access since memory access is always faster than disk access.

Cache in device RAM with overflow on hard disk

Write cache uses the VHDX differencing format:

- When RAM is zero, the target device write cache is only written to the local disk.
- When RAM is not zero, the target device write cache is written to RAM first. When RAM is full, the least recently used block of data is written to the local differencing disk to accommodate newer data on RAM. The amount of RAM specified is the non-paged kernel memory that the target device consumes.

Compared to "Cache on device hard drive" cache mode, the VHDX block format has a faster file expansion rate. The local disk free space is reconsidered to accommodate the streaming workload. To ensure target device reliability in a high demand workload, Citrix® recommends that local disk free space is larger than vDisk capacity size.

When the local disk is out of space, the target device vDisk I/O goes in to a pause state. It waits for more local disk free space to become available. This condition has a negative impact on the workload continuity. Citrix recommends allocating enough local disk free space.

The amount of RAM specified does not change the local disk free space requirement. The more RAM assigned, the more vDisk I/Os temporarily saved in RAM cache before all data gets flushed back to the VHDX file. The RAM reduces the initial VHDX expansion rate.

Cache on a server

Write cache can exist as a temporary file on a provisioning server. The Provisioning server handles all writes, which can increase disk I/O and network traffic.

For extra security, the server can be configured to encrypt write cache files. Since the write-cache file does exist on the hard drive between reboots, the data is encrypted in the event a hard drive is stolen.

Cache on server persistent

This cache option allows for the saving of changes between reboots. Using this option, after rebooting, a target device is able to retrieve changes made from previous sessions that differ from the read only vDisk image. If a vDisk is set to **Cache on server persistent**, each target device that accesses the vDisk automatically has a device-specific, writable disk file created. Any changes made to the vDisk image are written to that file, which is not automatically deleted upon shutdown.

The file name uniquely identifies the target device by including the target device's MAC address and disk identifier. A target device can be assigned to multiple vDisks and therefore have multiple cache files associated to it.

To restore a vDisk that uses **Cache Persistent on Server**, be sure to back up all vDisk files and associated user cache files before making changes.

The benefits of using this cache option include:

- Saves target device specific changes that are made to the vDisk image.
- Same benefits as standard image mode.

The drawbacks of using this cache option include:

- The cache file is available so long as the file remains valid. Any changes made to the vDisk force the cache file to be marked invalid. For example, if the vDisk is set to **Private Image Mode**, all associated cache files are marked invalid.

> **Note:**
>
> Cache files that are marked as invalid are not deleted. Periodically, these files are manually deleted.
>
> Invalidating changes include:

- Placing a vDisk in maintenance
- vDisk is placed in private image mode
- Mapping the drive from the Citrix Provisioning console
- Changing the location of the write cache file
- Using the automatic update

Tip:

Consider the impact of using a server-side persistent write cache. Persistent cache is only used where unauthorized users have access to a machine. Ensure that machines are not shared among users.

Selecting the write cache destination for standard virtual disk images

Citrix Provisioning™ supports several write cache destination options. However, the recommended option is cache in device RAM with overflow on the hard disk.

Note:

If migrating from older local hard disk caches to cache in device RAM with overflow to hard disk, you must reevaluate your local disk cache size. This is because the new RAM cache with overflow to hard disk uses a larger segment size and grows faster and larger.

The write cache destination for a virtual disk is selected on the **General** tab, which is available from the **vDisk File Properties** dialog.

The following sections describe all write cache destination options.

Cache in device RAM

Write cache can exist as a temporary file in the target device's RAM. This functionality provides the fastest method of disk access since memory access is always faster than disk access. The maximum RAM write cache size is determined by the registry setting `WcMaxRamCacheMB`.

Note:

- The target device becomes unstable and can crash if the target device's RAM write cache is full.
- For Windows 10 version 1803, the functionality *cache in device RAM* is not supported. A target device crashes when it fails to use reserved memory from bootstrap. Citrix® recommends using *Cache in device RAM with overflow on hard disk*. This issue applies to legacy bootstrap, it does not apply to UEFI bootstrap configurations.

Cache in device RAM with overflow on hard disk

This write cache method uses VHDX differencing format:

- When RAM is zero, the target device write cache is only written to the local disk.
- When RAM is not zero, the target device write cache is written to RAM first. When RAM is full, the least recently used block of data is written to the local differencing disk to accommodate newer data on RAM. The amount of RAM specified is the non-paged kernel memory that the target device consumes. Compared to Cache on device hard drive cache mode, the VHDX block format has a faster file expansion rate.

When the local disk is out of space, the target device virtual disk I/O goes in to a pause state. It waits for more local disk free space to become available. This condition has a negative impact on workload continuity. Citrix recommends allocating enough local disk free space.

The amount of RAM specified does not change the local disk free space requirement. The more RAM assigned, the more virtual disk I/Os temporarily saved in RAM cache before data gets flushed back to the VHDX file. The RAM reduces the initial VHDX expansion rate.

> **Tip**

> The registry setting `WcMaxRamCacheMB` is not used when configuring the **Cache in device RAM with hard disk overflow**. When using this write cache mode on the provisioning management console, the value specified from the maximum allocated size is used.

Cache on a server

Write cache can exist as a temporary file on a provisioning server. The server handles all writes, which increases disk I/O on the server and network traffic. For that reason, this mode is not recommended.

For extra security, the server can be configured to encrypt write cache files. Since the write-cache file does exist on the hard drive between reboots, the data is encrypted in the event a hard drive is stolen.

> **Note:**

> Consider the performance impact of using server side caching. This consideration applies to both persistent and non-persistent cache.

Support for replicated vDisk storage

Citrix Provisioning supports the replication of a vDisk on stores that are local, `local/attached` storage on provisioned servers, and contained within a site.

Replication considerations include:

- All Citrix Provisioning™ servers must have network connectivity with all other servers in the farm.
- Replication must be properly configured to function with Citrix Provisioning and meet all requirements.
- Replicated files include: `*.vhdx`, `*.avhdx`, and `*.pvp`. If you are importing existing vDisks, the `*.xml` manifest files can also be replicated. The `*.lok` files are not replicated.
- It is not necessary to shut down a server during the replication process.
- Store path must be set for each provisioning server.

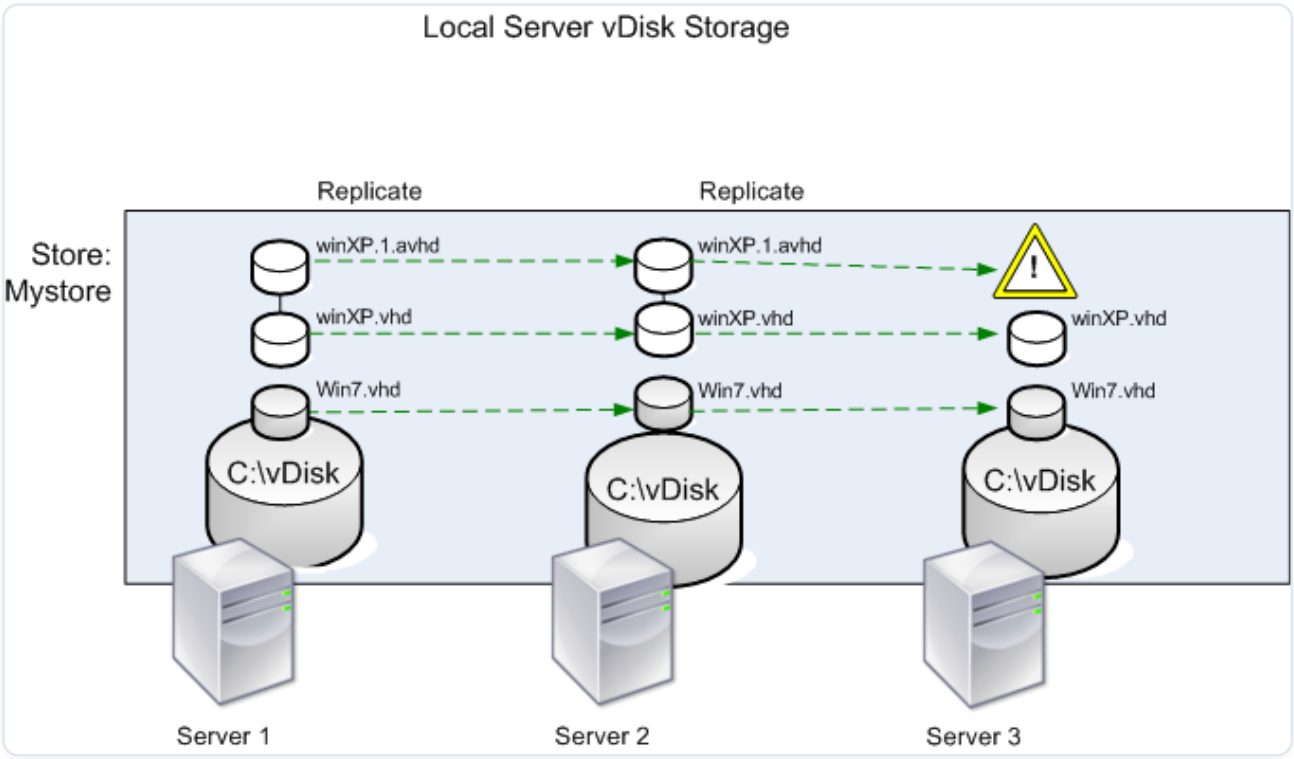
  > **Note:**
  >
  > If you are setting an override store path on the server's **Properties** dialog, the path must be set before creating a version of the vDisk. Because this path information is stored and referenced in the `.vhdx` header information, changing the path after versioning can cause unexpected results.

- Necessary storage must be available and have read/write access.

> **Note:**

> While DFS Replication can be used with Citrix Provisioning, DFS Namespaces are not supported as store paths.

> The following illustration shows a replication scenario where a version is not available to all servers from local storage.



The replication status can be viewed for a particular version of a vDisk or for all versions of a vDisk.

Troubleshooting and viewing replication status for a particular vDisk

Citrix Provisioning allows users to view the availability of replicated vDisks to provisioning servers within a farm.

1. Right-click on a vDisk in the Citrix Provisioning console, then select the **Versions** menu option. The **vDisk Versions** dialog appears.
2. Highlight a version in the dialog, then click **Replication**. The **vDisk Version Replication Status** dialog displays showing the replication status availability for each server that can provide this version of the vDisk.

    - If a version is in **Maintenance** (hammer icon), **Test** (magnifying glass), or **Pending** (hour glass) states, that state displays in the first row.
    - A **blue checkmark** indicates that the server has access to this version.
    - An **orange warning** indicates that a server currently does not have access to one or more versions of this vDisk. The version that is missing, or has an issue, has an orange warning under that version column.

Troubleshooting and viewing replication status for all versions of a vDisk

1. Right-click on a vDisk in the console, then select the **Replication Status** menu option. The **vDisk Version Replication Status** dialog appears.

2. The **Server** column lists all servers that can provide this vDisk and the general replication status of that server. The **Version** column lists each version of the vDisk and that versions individual replication status.

    - If a version is in **Maintenance** (hammer icon), **Test** (magnifying glass), or **Pending** (hour glass) states, that state displays in the first row.
    - A **blue checkmark** indicates that the server has access to this version.
    - An **orange warning** indicates that a server currently does not have access to one or more versions of this vDisk. The version that is missing, or has an issue, has an orange warning under that version column.

Exporting and importing vDisks

Citrix Provisioning™ exports and imports both *versioned* and *unversioned* vDisks from an existing store to another store in a different farm.

With vDisk versions, you can isolate updates to a vDisk or allow for quick revisions without affecting and copying a 30–40 GB file every time you want to make an update to your vDisk.

When working with vDisk versions, exporting the vDisk is the easiest way to move those versions to another farm. When you export a vDisk, an XML manifest file for the given vDisk is created. The XML manifest file fetches version details from SQL and/or the vhdx/avhdx files on vDisk. This can then be used to import the vDisk into the Citrix Provisioning console. An unversioned vDisk can be imported without the manifest XML file, but a versioned vDisk requires a manifest XML file before it can be imported.

> **Tip:**
>
> Merge differencing disks first to a base disk using third party tools if you are importing VHDs that are not exported using Citrix Provisioning. After merging them, import the new VHD base disk.

Exporting vDisks

To export a vDisk

1. Right-click on the vDisk in the Citrix Provisioning console, then select the **Export** menu option. The **Export** dialog appears.

2. Select the version to export from the menu, then click **OK**. The manifest file is created in the Store.

Tip:

If you delete a vDisk that you plan to export, Citrix® recommends that you export the vDisk first. After exporting it, copy the resulting XML file to the new location before deleting it from the original location.

Importing vDisks

A vDisk or vDisk chain of differencing VHD files can be imported into a store if:

- The imported VHD does not exist in the store and both the highest version number of the VHD and associated manifest files match.
- The VHD chain includes a base image, and that base image version number matches the base image version in the manifest file.

Note:

When importing a single vDisk, no manifest file is required, however, if you import vDisks with versions you must include a manifest file.

- The VHD does exist in the store but the imported version number in the associated manifest file is greater than the existing VHD version number.

Important:

If you have an existing vDisk with the same name in other stores, and one or more of those stores either has not set the provisioning server, or the server is unreachable, the import fails. A message appears to indicate *No server available to handle* . This issue occurs because the import process checks that the imported vDisk is not stored in the same location as the vDisk with the same name in the other store.

To add or import an existing vDisk to a site

1. Copy the vDisk and any associated properties files to shared storage, if they do not exist there.
2. In the console, right-click on the **Store or a vDisk Pool**, then select the **Add or Import Existing vDisk** menu option. The **Add or Import Existing vDisks** dialog appears.
3. Select the store to search for vDisks from the **Store to search** menu.
4. Select the server to use to search for vDisks from the **Server to use for searching** menu, then click **Search**. All vDisks in the store display in the **Add checked vDisks to the vDisk Pool**.
5. Check the vDisks you want added to the vDisk pool.
6. Optionally, check **Enable load balancing for these vDisks** to enable load balancing on provisioning servers that provide this vDisk to target devices.
7. Click **Add** to add the vDisk(s) to the vDisk pool.

Adding vDisk versions

To add a vDisk version to a site

1. Copy the vDisk, and any associated property files, to shared storage, if they do not exist there.
2. In the console, right-click on the **Store** or a **vDisk Pool**, then select the **Add vDisk Versions** menu option. The **Add vDisk Versions** dialog appears.
3. Select the store to search for vDisks from the **Store to search** menu.
4. Select the server to use to search for vDisks from the **Server to use for searching** menu, then click **Search**. All vDisks in the store display in the **Add checked vDisks new versions**.
5. Check those vDisk versions added to the vDisk pool.
6. Click **Add** to add the vDisk(s) to the vDisk pool.

Releasing vDisk locks

Multiple target devices and Citrix Provisioning™ servers access a single vDisk image file, which makes it necessary to control access to prevent corruption of the image. When a user accidentally assigns a private image to multiple target devices, and then tries to boot those target devices, a corrupt image results. Therefore, the image becomes locked appropriately for a given configuration. The locked vDisk icon appears with a small *lock* on it.

Under certain circumstances these locks are not released properly. A lock on a vDisk image is not released properly when:

- a target device machine is booted from a vDisk, and then

- shuts down without running through the normal shutdown process. For example, if the VM crashes or the hypervisor stops the VM without waiting for orderly shutdown to complete.

If the same target device boots again, the same lock is used and no problem occurs. However, if an administrator tries to mount the drive on the provisioning server after the target device has failed, the server fails to mount that vDisk. The server fails to mount the vDisk because a lock is still held by the failed target device. The administrator can release these locks.

> **Note:**
>
> Ensure that the vDisk is not in use before removing a lock. Removing a lock for a vDisk, which is in use, might corrupt the image.

To release vDisk locks

1. In the Citrix Provisioning console, right-click on the vDisk for which you want to release locks, and then select the **Manage Locks** option. The **Manage VDisk Locks** dialog appears.
2. If a vDisk has a target device lock on it, that target device name appears in the dialog's list. Select one or more target devices from the list, then click **Remove lock**. You can also choose **Select All** to remove all target device locks on the selected vDisk.
3. Click **Close** to close the dialog.

Copying and pasting vDisk properties

Use the **Copy** and **Paste** options to copy properties of one vDisk to one or more vDisks in your network.

To copy vDisk properties to one or more vDisks

1. In the Citrix Provisioning™ console, right-click on the vDisk that has the properties settings that you want to share with other vDisks. Select **Copy vDisk Properties**. The **Copy vDisk Properties** dialog appears.
2. Select the check boxes next to the properties that you want to copy to other vDisks, then click **Copy**.
3. In the details panel, highlight the vDisks that you want to paste properties settings to, then click **Paste** from the right-click menu.

Adding existing vDisks to a vDisk pool or store

If vDisks exist in a store, and are used by target devices in your site, you can add them to the site's vDisk pool. In the Citrix Provisioning™ console, select **Add existing vDisks** by right-clicking the menu option. This option is available from the **vDisk Pool** folder and from a store folder.

To add existing vDisks to a site

1. Verify the following:
    - Other servers have access to the shared folder where the store is located.
    - The new server is associated with that store.
2. In the console tree, right-click on the **vDisk Pool** in the site where you want to add vDisks. You can alternately right-click on the store where those vDisks exist. Select the **Add existing vDisk** menu option. The **Add Existing vDisks** dialog appears.
3. If you accessed this dialog from the site's vDisk pool, select the store to search from the menu. If you accessed this dialog from the store, select the site where vDisks are added using the menu.
4. In the **Select the server to use when searching for new vDisks** menu, select the Citrix Provisioning server performing the search. Click **Search**. Any new vDisks that do not exist in the database display in the text box.
5. Check the box next to each vDisk that you want to add. Alternately click **Select All** to add all vDisks in the list, then click **Add**.

Backing up a vDisk

The Citrix Provisioning™ server treats a vDisk image file like a regular file, but the target device treats it as a hard drive. The procedure for backing up a vDisk image file is the same as backing up any other file on your server. If a vDisk image file becomes corrupt, restoring it requires replacing the corrupted file with a previous, functional version.

> **Note:**
>
> Do not back up a vDisk while its being used or while it is locked. Citrix® recommends backing up these disks using your normal provisioning server backup routine.

Viewing vDisk usage

To view target devices that are connected to a specific vDisk

1. Right-click a vDisk in the Citrix Provisioning™ console, then select the **Show usage** menu option. The **Show vDisk Usage** dialog appears.
2. Select one or more target devices in the list to perform any of the following target device connection tasks:
    - Shut Down – shuts down the target device.
    - Reboot – reboots the target device.
    - Send Message – opens the **Edit Message** dialog to allow you to type, and then send a message to target devices.

To view all target devices served by a Citrix Provisioning server

1. Right-click on a Citrix Provisioning server in the console, then select the **Show Connected devices** menu option. The **Connected Target Devices** dialog appears.
2. Select one or more target devices in the list to perform any of the following target device connection tasks:
    - Shut Down – shuts down the target device.
    - Reboot – reboots the target device.
    - Send Message – opens the **Edit Message** dialog to allow you to type, and then send a message to target devices.

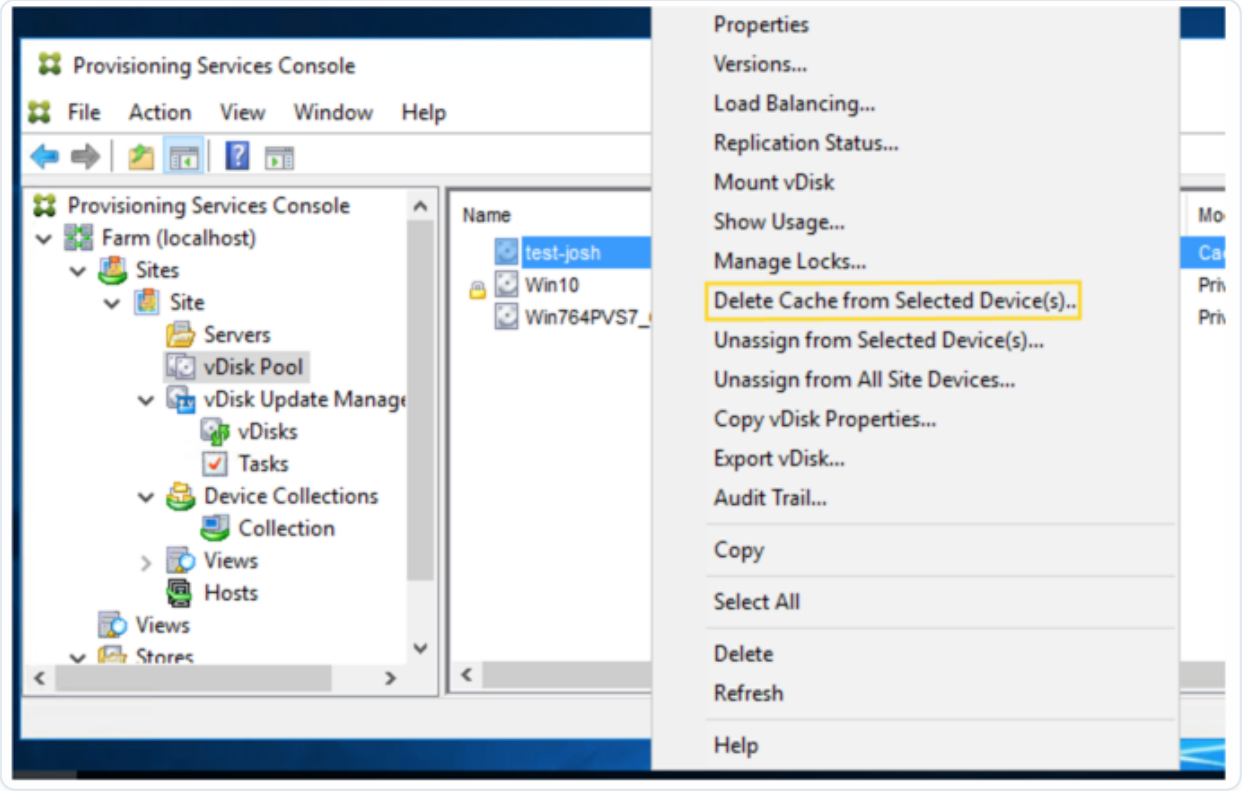
Deleting cache on a difference disk

The **Delete Cache from Selected Devices** context menu option manually deletes the cache on a difference disk. It is only available if the vDisk cache mode is set to **Server Persistent Cache**.

> **Note:**
>
> The write cache on a difference disk is not automatically deleted if that file becomes invalid. Citrix® recommends manually deleting files marked as *invalid*.

To delete a cache on a difference disk

1. In the Citrix Provisioning™ console, right-click on the vDisk that is associated with difference disk files you want to delete. Select the **Delete Cache from Selected Devices** menu option.



   The **Delete Cache for Devices** dialog box appears.

2. Check each target device cache you want to delete, or click **Select all** to delete all cache files associated with this vDisk.
3. Click **Delete** to delete the cache files from the server.

Assigning vDisks and versions to target devices

A vDisk version can be assigned and unassigned to a target device.

Accessing a version of the vDisk

Numerous differencing disk versions can exist for a vDisk. Device access to a particular version, or the ability to make updates to that version, depends on that versions **access mode** setting and the **device type**. The sections that follow describe the different version access modes and device types and their relationship to each other.

A version's access mode is managed on the vDisk **Versioning** dialog. New versions of a vDisk are promoted from **Maintenance** to **Test** and then into **Production**. Access mode options include:

- **Maintenance** – new read/write difference disk version that is only available to the first Maintenance device that selects to boots from it to make updates.
- **Test** – read-only version used for test purposes and only available to Test or Maintenance devices.
- **Pending** – read-only version and not yet available for use by production devices. This field indicates that the scheduled release date and time have not been reached. Or, the version is not yet available to all servers in the site. If the **Boot production devices** option is set to **Newest released**, the default changes. After the release date and time is reached and all servers are able to access this version, access changes to *default*. If the access display is blank, this version is considered released to production. However, it is not the version currently selected as the version from which production devices boot.
- **Default** – read-only version that is bootable by all device types. The latest released production version is marked with a green checkmark if the **Boot production device from version** is set to **Newest released**. The status is set to default.
- **Override** – read-only version that is bootable by all device types. If a specific version is selected from the **Boot production devices** from the version menu, that version is marked with a green checkmark. Access changes to **Override**.
- **Newest released** – read-only version that is bootable by all devices. If a specific version is selected from the **Boot production devices** from the version menu, that version is marked with a green checkmark. Access changes to **Override**.
- **Merging** – a merge is occurring to this new version. This version is unavailable to all device types until the merge completes. After the merge completes, the status of the new version depends on the **Access mode** selected on the **Mode to set the vDisk to after automatic merge** menu. Modes are production, maintenance, or test. This **Farm Properties** setting is available on the **vDisk Versions** tab.

Device types

The device type is selected on the Target Device Properties **General** tab, unless it is an update device, which is created automatically along with the managed vDisk.

Device types include:

- **maintenance devices**

  Maintenance devices can access any available version of a vDisk. A maintenance device's primary role is to manually update a vDisk. To manually update a disk, you request a new version from the vDisk **Versions** dialog. This process creates a differencing disk and places

that newly created version in **Maintenance Access** mode. While in maintenance mode, this version of the vDisk is solely accessed by a single maintenance device, which is the first maintenance device that accesses it. Using that device, the vDisk is booted and any updates that are made are captured in the new differencing disk version. After updates are complete, the maintenance version can be promoted to Test mode or directly to production mode.

> **Note:**
>
> In **Maintenance Mode**, a new version can also be created by merging existing versions into a new version or new base disk image.

- **test devices**

  While in Test mode, the vDisk version can only be streamed to test or maintenance devices to which it is assigned. Streaming in this mode allows the new version to be tested before being released into the production environment. And it permits production devices to continue to stream from the previous version without interruption. If issues are found, this version can be reverted into maintenance mode.

- **production devices**

  After you successfully test the new version, it can be promoted to production mode and made available to product, test, and maintenance devices to which it is assigned. If issues are found, this version can be reverted into either test or maintenance mode. This process only occurs after booted devices accessing this version are shut down.

  If a device is assigned a vDisk, after the updated disk is tested you can change the device to be a vDisk production device. This cofiguration allows you to continue testing for compatibility within your production environment.

  - **update devices**

  Update devices are used to update a managed vDisk, which is created automatically when running the **Managed vDisk Setup Wizard**. Only one updated device exists for each managed vDisk, and that disk and that updated device are given the same name. For more information on managed vDisks, see *vDisk Update Management*.

Unassigning a vDisk from target device

To unassign a vDisk from a target device:

1. Select the vDisk in the Citrix Provisioning™ console, then right-click and select the **Unassign from Selected Devices** or **Unassign from All Site Devices** menu option.
2. If unassigning from select devices, in the **Unassign from Devices** dialog, select the devices to unassign to this vDisk, then click **Unassign**. If unassigning from all devices in a site, click **Yes** on the confirmation dialog that appears.
3. After the target devices are successfully unassigned, close any open dialogs.

> **Note:**
>
> The **Unassign from All site Devices** option only unassigns vDisks that are not personal vDisks.

vDisk versioning dialog

vDisk versioning is managed from the **vDisk Versions** dialog. To open the dialog, right-click on a vDisk in the console, then select the **Versions...** menu option. The following provides a general description of the **vDisk Versions** dialog:

- Boot production devices from version

  From the menu box, select the version to use when booting target devices in production. The default is the newest version.

- Version and status

  This column lists versions and the status of each version:

  - the wrench icon indicates that this version's access mode is set to *Maintenance* mode. Only a single maintenance device can boot.
  - the magnifying glass icon indicates that this version's access mode is set to *Test*. Only a test device can boot.
  - the clock icon indicates that this version's access mode is set to *Pending*. A version that is Pending has been promoted to production but the release date and time have not yet been reached.
  - the green checkmark icon indicates that this version is the current production version based on settings selected on the **Boot production devices from version** menu. All device types can boot from vDisk version that is in production.

    - the red X icon indicates that this version is obsolete, no devices are currently booted from it, and that this version can be deleted because a merged base was created, which is more current.

- Created

  Provides the date and the time that this version was created. Date format is YYYY/MM/DD and time format is HH:MM

- Released

  Provides the date and time that this version is scheduled for release to production. The date format is YYYY/MM/DD and time format is HH:MM

- Devices

  The number of target devices streaming sessions for a given version.

- Access

  Indicates target device access availability for a given version.

  Maintenance read/write version that is available to the first maintenance device that selects to boots from it.

  Test read-only version used for test purposes and only available to test or maintenance devices.

  Pending read-only and not yet available for use because the scheduled release date and time have not been reached.

  Default read-only version that is bootable by all devices. If the **Boot production devices from version** is set to **Newest released**, the latest released production version is marked with a green checkmark. Access is set the **Default**.

  Override read-only version that is bootable by all devices. If a specific version is selected from the **Boot production devices from version** menu, the access changes to **Override**.

  Merging a merge is occurring to this new version. This version is unavailable until the merge completes. After the merge completes, the status of the new version depends on the access mode selected on the Mode to set the vDisk to after automatic merge menu (Production, Maintenance, or Test). The default **Farm Properties** setting is available on the **vDisk Versions** tab. A wrench icon appears for the merging version.

  Blank, indicates that this version was released to production.

- Type

  Identifies how the vDisk was created. The options include:

  - Manual created using Maintenance mode.
  - Automatic created automatically using an automated update.
  - Merge Created by a partial merge operation.
  - Merge Base Created by a base merge operation (no parent needed).
  - Base The original base image.

- New

  Creates a maintenance version.

- Promote

  Opens a dialog that prompts to promote this version to Test or Production. If Production is selected a release date and time can be set or the default (now) can be accepted.

- Revert

  Reverting from Test version: if no maintenance access version exists, revert moves latest test version into Maintenance.

  Reverting from Production: any booted device is shut down before reverting. Clicking **Revert** opens a dialog that allows the user to select to revert to test or maintenance.

- Delete

  Clicking **Delete** opens a delete confirmation dialog. Click **OK** to delete the selected version. Delete is only available if the latest version or obsolete version doesn't have target devices currently booted from it.

- Replication

  Selecting a version, then clicking **Replication** opens the **Disk Versioning Replication Status** dialog. This dialog displays the replication status of this version on each server:

  - Blue check next to the server name indicates that the version has been replicated on the server.
  - Orange triangle next to the server name indicates that the version has not yet been replicated or there is an issue. Placing the cursor over the triangle displays the related error message.

To view the replication status of all versions of this vDisk on each server, right-click on the vDisk in the console, then select **Replication Status** from the context menu.

- Properties

  Clicking the **Properties** button opens the **vDisk Version Properties** dialog, which allows you to enter a description related to this version. It also displays availability of a selected version if that version is set for release to production in the future. Or, if no device has booted from that version.

- Text

  The text box provides a description of the currently selected version.

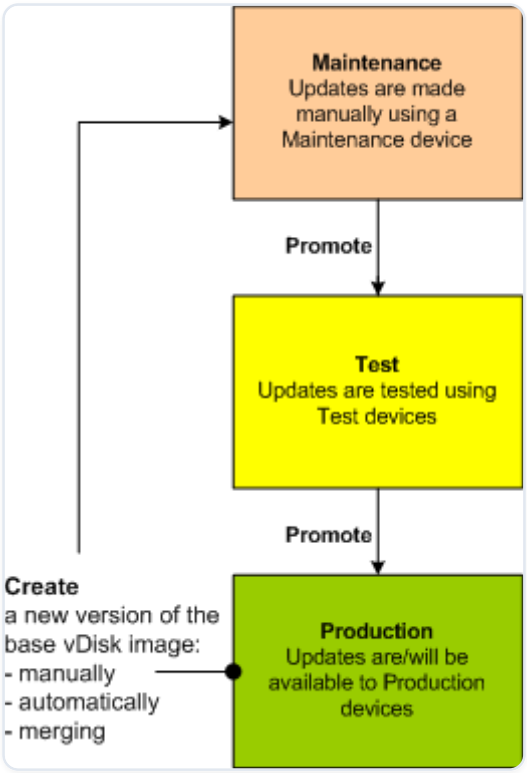
Updating vDisks

It is often necessary to update an existing vDisk so that the image contains the most current software and patches. Each time the vDisk is updated, a new version of that vDisk is created. This file is seen as a Hyper-V Virtual Hard Drive, with the extension `.vhdx`. This new version is used to capture the changes without updating the base vDisk image.

Updating a vDisk involves the following:

- Create a version of the vDisk, manually or automatically.
- Boot the newly created version from a device (maintenance device or update device), make and save any changes to the vDisk, then shut down the device.
- Promote the new version to production.

The following illustrates the general promotion of a vDisk update:



The availability of the updated version depends on the current promotion of that version, for example, maintenance, test, or production. It also depends on the type of device attempting to access it, for example, maintenance device, update device, test device, or production device.

Update scenarios

The following vDisk update scenarios are supported:

- **Manual Update** – Manually update a vDisk by creating a version; use a *Maintenance* device to capture updates to that version. On the **vDisk Versions** dialog, initiate a manual update by clicking **New**. The **Access** column on the **vDisk Versions** dialog indicates that the newly created version is in maintenance. A single maintenance device updates this version while in maintenance mode. Multiple maintenance devices can be assigned to a vDisk. However, only one device can boot and access that version of the vDisk at any given time. During that time that maintenance device has exclusive read/write access.
- **Automated Update** – Creating automated updates saves administration time and physical resources. Updates are initiated on-demand or from a schedule and are configured using vDisk Update Management. If you are updating automatically, the **Access** column on the **vDisk Versions** dialog indicates that the newly created version is in maintenance. The device to which it is assigned is updated while in maintenance mode, where only one update device exists per vDisk.

> **Note:**

> vDisk Update Management is intended for use with standard image mode vDisks only. Private image mode vDisks can be updated using normal software distribution tool procedures. Registering a vDisk in private image mode for update management, or switching a vDisk that is already registered, generates errors.

- **Merge** – Merging VHDX differencing disk files can save disk space and increase performance, depending on the merge option selected. A merge update is initiated manually by selecting the **Merge** button on the vDisk Versions dialog, or automatically when the maximum vDisk versions count is reached.

VHDX chain of differencing disks

Versioning simplifies vDisk update and management tasks, providing a more flexible and robust approach to managing vDisks.

A vDisk consists of a VHDX base image file, any associated side-car files, and if applicable, a chain of referenced VHDX differencing disks. Differencing disks are created to capture the changes made to the base disk image, leaving the original base disk unchanged. Each differencing disk that is associated with a base disk represents a different version.

The following sections discuss the file naming convention used and the relationship between a base disk and all versions referencing it.

VHDX chain

> **Note:**
>
> vDisk versions are created and managed using the vDisk **Versions** dialog and by performing common vDisk versioning tasks.

> Each time a vDisk is put into maintenance mode a new version of the VHDX differencing disk is created. The file name is numerically incremented. The following table illustrates these chain sequences:

	VHDX FILE NAME	PROPERTIES FILE NAME	LOCK FILE FILE NAME
Base Image	win7dev.vhdx	win7dev.pvp	win7dev.lok

	VHDX FILE NAME	PROPERTIES FILE NAME	LOCK FILE FILE NAME
Version 1	win7dev.1.avhdx	win7dev.1.pvp	win7dev.1.lok
Version 2	win7dev.2.avhdx	win7dev.2.pvp	win7dev.2.lok
Version 3	win7dev.3.avhdx	win7dev.3.pvp	win7dev.3.lok
Version 4	win7dev.4.vhdx	win7dev.4.pvp	win7dev.4.lok
Version N	win7dev.**N**.vhdx	win7dev.**N**.pvp	win7dev.**N**.lok

For Version 4 and Version N merged base VHDX and AVHDX files are combined and use the VHDX extension.

Manually updating a vDisk image

Use the vDisk Versions dialog to create a version of the vDisk's base image.

> **Note:**
>
> To automate an update process, configure for vDisk update management. See Automating vDisk Updates.

This procedure requires that:

- A maintenance device has been assigned to the vDisk being updated.
- No version of this vDisk is under maintenance.

Create a version

1. In the Citrix Provisioning™ console, right-click on a vDisk to version within a device collection or vDisk pool, then select **Versions** from the context menu. The **vDisk Versions** dialog appears.

   > **Note:**
   >
   > Verify that the vDisk is not in private image mode.

2. Click **New**. The new version displays in the dialog. Access set to *maintenance* and the update type method set to *manual*.
3. Boot the vDisk from a maintenance device, install or remove applications, add patches, and complete any other necessary updates, then shut down the maintenance device. Optionally, test that changes were made successfully.

   > **Note:**
   >
   > When booting a test or maintenance device, use the boot menu to select from the vDisk, or version of that vDisk, from which to boot.

4. Select the vDisk, then right-click. Select the **Promote...** menu option from the context menu that appears. For more details on promoting versions see Promoting Updated Versions.
5. Select to promote this maintenance version into test or directly into production. If **Production** is selected, set the availability of this version in production to be either immediate or scheduled.
6. Click **OK** to promote this version and end maintenance.

Merging VHDX differencing disks

Merging VHDX differencing disk files can save disk space and increase performance, depending on the merge method selected. Once a vDisk reaches five versions, Citrix® recommends merging the versions either to a new base image or to a consolidated differencing disk.

Merge methods include:

- Merging to a new base image
- Merging to a consolidated differencing disk

> **Note:**
>
> A merged vDisk only occurs when a maintenance version is not defined, or when it is in private image mode. A merged vDisk starts from the top of the chain down to the base disk image. A starting disk cannot be specified for the merged vDisk.

Merging to a new base image

Fully merging to a new base image combines a chain of differencing disks and base image disks into a new single base disk, which represents the next version in the chain with the file name extension `VHDX`. This method allows for the fastest disk access to the base image. Citrix recommends this process when performance is more important than disk space. Consider that a new base disk is created for every merge performed.

> **Tip:**
>
> After merging the base operation on a vDisk utilizing the VHDX file format, the merged base VHDX file is smaller than the original base VHDX file. This behavior occurs when files are deleted in a particular vDisk version. These files are no longer available in the merged base VHDX. For more information, see the Citrix Knowledge Center.

Merging to a consolidated differencing disk

A partial merge combines a chain of VHDX differencing disks up to, but not including, the base disk into a new differencing disk. The new differencing disk has the same parent base disk image. It is given the extension `avhdx`. This method consumes less disk space than the full merge and the merge process is quicker than performing a full merge.

Automatically consolidate differencing disks in the **Farm Properties** dialog's vDisk **Version** tab. Select a maximum vDisk number, when that number is reached, a merge is automatically performed. The availability of that vDisk depends on the mode selected on the tab, production, maintenance, or test.

> **Note:**
>
> Citrix recommends consolidating a merged differencing disk when storage is limited or when the bandwidth between remote locations is limited. These scenarios make copying large images impractical.

Merging differencing disks

1. Right-click on a vDisk in the Citrix Provisioning console, then select the **Versions** menu option. The vDisk **Versions** dialog appears.
2. Click the **Merge** button. The **Merge** dialog appears.

3. Select to perform **Merged Updates** or a **Merged Base** merge.
    - To merge all differencing disks to a single differencing disk (not to the base disk image), select the **Merged Updates** option.
    - To merge all differencing disks into a new base disk, select the **Merged Base** option.
4. Select the access mode, production, maintenance, or test, for this version after the merge completes. If an access mode is not selected, the vDisk mode defaults to **automatic range**, specified in the **Farm Properties** vDisk **Version** tab.
5. Click **OK** to begin the merge process.

The time it takes to complete the merge process varies based on the merge method selected and the number of differencing disks to merge. After the merge successfully completes, the new version displays in the vDisk Versions dialog. If you selected a full merge, the **Type** column displays either *Merge Base*, or *Merge* if a partial merge was selected.

Promoting updated versions

An updated version of the vDisk is not available to production devices until it is promoted to production. The update promotion stages include:

- maintenance
- test
- production

Each time a new version is created, the **Access** setting is automatically set to **Maintenance**, allowing maintenance devices to make updates. After you finish update, this version can be promoted from **Maintenance** to **Test** for read-only. This permits testing by test devices, or promotion directly to production, for use by all target devices.

After you complete an update using the manual method, the new version can be promoted to test or production from the vDisk Version dialog's **Promote** button. If you selected production, a release date and time can be set, or accept the default, *Immediate*.

After you complete an update using the automated update method, the new version is promoted according to the **Post Update** setting. After completing the automatic update, promote the version using the **vDisk Version** dialog's **Promote** button.

If issues exist in the new version, revert from test to maintenance, if no active sessions exist. You can alternately revert from production to either test or maintenance. Shut down any booted device before reverting to another version.

In order for production devices to access the new version after it is promoted to production, the following also applies:

- Access setting must be either **Default** or **Override**.
- If the update was scheduled for release, the date and time must be reached.
- The updated version must be available to all servers in the site.
- Boot production devices from a version set to **Newest released** on the **vDisk Versions** dialog.

> **Note:**
>
> When the **Access** field is blank, this version is considered released to production, however, it is not the version from which devices boot.

Updating vDisks on target devices

This article describes how to change a vDisk on multiple target devices without having to manually reconfigure them. It provides some general information about the process, then sets out a step-by-step procedure.

Setting vDisk class and type properties

For an automatic update to take place, the class of the target device and vDisk must match. For a newer vDisk to replace an older vDisk within a target device, the vDisk class and type of both vDisks must match. Multiple, duplicate vDisk instances can exist within your implementation. vDisks can be assigned to one or more target devices. For example, for the Citrix Provisioning server, **Least Busy** and **First Available** boot behaviors. Further qualify the old vDisk that replaced by the new vDisk.

> **Tip:**
>
> Never assign more than one vDisk with the same *type* from the same provisioning server to the same target device. This process applies to environments using the **Automatic Disk Image Update** feature.

Scheduling vDisk updates

Use the **Apply vDisk updates** to schedule updates. These updates are applied when detected by the server. You can alternately select **Schedule the next vDisk update** on the **Auto Update** tab of

the vDisk. If you select **Schedule the next vDisk update**, you must specify the current date or a later date. Failing to do so prevents an update to the vDisk.

Timed update of vDisks

You can set a timer to update vDisks. The vDisk are assigned to all the devices with a matching class at a specified time, for example when devices are less active.

To set a timer, create a Windows timer on one of the servers from each site. This process calls the PowerShell `Mcli-Run ApplyAutoUpdate` command or the `Mcli Run ApplyAutoUpdate` command. The command scans the site and updates all eligible vDisks. The timer executes every day. These updates are automatically made whenever you add new disk versions.

Automatically adding a replacement vDisk

To add a replacement vDisk to a site automatically, place it in the store directory of the vDisk it replaces. When the update process is done, each store for the site is scanned for vDisks that are not defined in the site. A vDisk is automatically added to a site and assigned to a target device with a matching class:

- if a vDisk is found with the same *Class* and *Type* as an existing vDisk in the store directory.
- if a vDisk is labeled as major or minor, and the build number is higher than the existing vDisk.

The replacement vDisk must include all versions since and including the last merged base, or if no merged base exists, the base. All the VHDX, AVHDX, and the PVP files for the included versions must be in the store directory.

If the replacement vDisk has multiple versions, the manifest (XML) file must be included with the vDisk. To create the manifest file, perform a vDisk Export. To reduce the number of delivered files, delete obsolete versions in the **vDisk Versions** dialog before performing exporting the vDisk.

Automatically update a vDisk

1. For the original vDisk, select the **Auto Update** tab, then set the following vDisk properties:

   a. Enable automatic updates.

   b. Run the `ApplyAutoUpdate` to determine if the update is immediately applied, or on a scheduled date.

   c. Enter a class and type for the vDisk.

   d. Enter a major, minor, and build number for the vDisk.

> **Note:**
>
> The **Serial Number** field is set to a random **Globally Unique Identifier (GUID)** when the vDisk is created. It is for information only and you can edit it. It is not used for processing the automatic update.

2. For target devices using the updated vDisk, select the **General** tab. In **Target Devices Properties** set the Class equal to the value of the original vDisk.
3. Ensure that the replacement vDisk is in the same store as the original vDisk.
4. For the replacement disk, select the **Auto Update** tab, set the following vDisk properties:

   a. Only enable automatic updates if this vDisk replaces another vDisk.

   b. If automatic updates are enabled, determine if the update is immediately applied. You can alternately schedule when to check for updates by running **ApplyAutoUpdate**.

   c. Enter the same class and type that you entered for the original vDisk.

   d. Enter a major, minor, and build number for the vDisk that is higher than the original vDisk.
5. If the vDisk update is required for other farm sites, deliver the replacement vDisk to them. Follow the information described in step 4. This updated vDisk is required in the same store as the original vDisk of the other farm site. See ‘Automatically adding a replacement vDisk’ earlier in this article.
6. Configure the update check. Updated vDisks contain a higher major, minor, and build number that are eligible using one of the following ways:

   - Right-click on the vDisk Pool, select the **Check for Automatic Updates** menu option, then click **OK** on the confirmation dialog.

     Or

   - Set a timer as described earlier in this article.

Automating vDisk updates

vDisk update management is intended for use with **Standard Image Mode** vDisks only. Private image mode vDisks are updated using normal software distribution tool procedures. Attempting to register a private image mode vDisk for vDisk update management, or switching a vDisk that is already registered, causes errors. In the console, the **vDisk Update Management** feature is used to configure the automation of vDisk updates using virtual machines (VMs). Automated vDisk

updates occur on a scheduled basis, or at any time that the administrator invokes the update directly from the console. This feature supports updates detected and delivered from WSUS and SCCM Electronic Software Delivery (ESD) servers.

When the Site node is expanded in the console tree, the vDisk Update Management feature appears. When expanded, the vDisk Update Management feature includes the following managed components:

- Hosts
- vDisks
- Tasks

Configuring a site for vDisk Update Management requires the following:

1. Designate a provisioning server within the site to process updates. See Enabling Automatic vDisk Updates.
2. Configuring a virtual host pool for automated vDisk updates. See Using the Virtual Host Connection Wizard.

   > **Note:**
   >
   > Supported hypervisor types include XenServer (formerly Citrix Hypervisor), Microsoft SCVMM/Hyper-V, VMware vSphere/ESX, and Nutanix.

3. Create and configure an ESD VM that used to update the vDisk. See Creating and Configuring ESD Update VMs.
4. Configuring vDisks for automated updates. See the Using the Managed vDisk Setup Wizard.
5. Creating and managing update tasks. See Using the Update Task Wizard.

   > **Note:**
   >
   > The user that configures vDisk update management tasks must have permissions to create, modify, and delete Active Directory accounts.

6. Run the update task by right-clicking on the task object in the console, and then selecting the **Run update now** menu option. The update VM boots, install updates, and reboot as

necessary. After the update task successfully completes, the virtual machine is automatically shut down. The update status can be checked from the console tree under **vDisk Update Management>vDisks>(vDisk name)> Completed Update Status**. The status can also be checked using the event viewer or in WSUS.

After configuring the site to use vDisk update management, managed vDisks are updated using the following methods:

- Scheduled – the image update service automatically updates a vDisk, on a scheduled basis as defined in the Update Task.
- User Invoked – select a managed vDisk from the Console's **Run update now** menu option. This option requires you to manually start, then stop the Update Device after the update is complete.

Consider the following when automating vDisk updates:

- The vDisk update process starts either automatically (scheduled), or when an administrator right-clicks on a managed vDisk, then selects the **Run update now** menu option.
- Citrix Provisioning creates a version (VHDX) and places that version in maintenance mode (read/write).
- The virtual machine boots the assigned vDisk. If **Scheduled update** is configured, vDisk update management performs the boot automatically. For a **User invoked update**, the administrator invokes the update.
- All updates are automatically made and captured in the new version of the VHDX file.
- After you update the vDisk, the virtual machine is shut down automatically.
- The vDisk is promoted from maintenance to either test or production. The availability of the new vDisk version depends on the access mode that was selected when the **Update Task Wizard** was run. Or, when the mode is selected on the **Update Task** Properties' **Finish** tab (maintenance, test, or production). After this version is made available in production, target devices will be able to access it the next time they boot that vDisk.

Enabling automatic vDisk updates

To enable automatic vDisk updates:

1. Right-click on the Site in the console, then select the **Properties** menu option. The **Site Properties** dialog appears.
2. On the **vDisk Update** tab, check the box next to **Enable automatic vDisk updates on this site**.

3. Select the server to run vDisk updates for this site, then click **OK**.

Managed vDisks can now be automatically updated on this site. Next, virtual host connections must be configured to allow for automatic updates to be made. See Configuring Virtual Host Connections for Automated vDisk Updates.

Configuring virtual host connections for Automated vDisk updates

When you use vDisk update management, a designated hypervisor server is selected from within a virtual pool that is then used to communicate with Citrix Provisioning. Create the designated hypervisor by running the Virtual Host Connection Wizard. If you are running a vCenter server on alternate ports, the following registry modifications must be made to connect to it from Citrix Provisioning:

- Create a registry key named **PlatformEsx** under **HKLM\Software\Citrix\Citrix Provisioning**
- Create a string value in the **PlatformEsx** key named ServerConnectionString and set it to `http://{0}:PORT#/sdk`. If you are using port 300, `ServerConnectionString=http://{0}:300/sdk`.

To configure virtual host connections:

1. Under the **vDisk Update Management** node in the Citrix Provisioning console, right-click on **Hosts**, then select the **Add host...** option. The **Virtual Host Connection Wizard** appears.
2. Click **Next** to begin. The **Hypervisor** page appears.
3. Click the radio button next to the type of hypervisor used by this pool, then click **Next**. Options include Citrix XenServer, Nutanix, SCVMM/Hyper-V, or vSphere/ESX. The **Name/Description** page appears.
4. Enter the name, and optionally a description, for the **Virtual Host Connection** then click **Next**.
5. Enter the host name or the IP address of the server to contact. If an ESX hypervisor was selected, optionally specify the data center to use when connecting to the host. Note: It can take several minutes before a hostname/IP address can be reentered, if that hostname/IP was previously entered and then deleted.
6. Click **Next**. The **Credentials** page appears.
7. Enter the appropriate credentials required to connect to this host, then click **Next**. Specify the following: User name – the account name with appropriate permissions to access the virtual host pool server. Password – password used with this account name. The password must be a maximum of 32 characters. The **Confirmation** page appears.

8. Review the settings to ensure accuracy, then click **Finish**. **Virtual Host Pool** properties can be viewed or modified on the **Virtual Host Connection Properties** dialog.

General tab

FIELD	DESCRIPTION
Type	The type of virtual host connection that was selected when the Virtual Host Connection Wizard was run. This field cannot be modified.
Name	The name to use when referencing this virtual host connection by Citrix Provisioning.
Description	A brief description of this virtual host connection.
Host	The host name or IP address of the virtual host connection server used by Citrix Provisioning. To use a different port for the ESX server connection, in the server address field, enter the full connection string and include the correct port number. The format for the connection string is `http://server_name:port/sdk`. **Note:** If you are running a vCenter server on alternate ports, the following registry modifications must be made to connect to it from Citrix Provisioning: Create a new key `HKLM\Software\Citrix\CitrixProvisioning\PlatformEsx`. Or, create a string in the **PlatformEsx key** named *ServerConnectionString* and set it to `http://{0}:PORT#/sdk`. If you are using port 300, `ServerConnectionString= http://{0}:300/sdk`.
Data center	Optional. If an ESX hypervisor was selected, optionally specify the data center to use when connecting to the host.

Credentials tab

FIELD	DESCRIPTION
Update limit	The account user name required to connect to the virtual host server.
Password	The account password that is associated with the user name. The password must be a maximum of 32 characters.
Verify Connection Button	Click this button to verify that the user name and password entered are valid and allow communications to the virtual host pool server.

Advanced tab

FIELD	DESCRIPTION
Update limit	Controls the number of virtual machines that can concurrently process updates. Any additional updates are queued and start as virtual machines complete processing.
Update timeout	The maximum amount of time allowed to perform an update to an image. If the update has not completed before the timeout period, the update is canceled.
Shutdown timeout	The maximum amount of time to wait for the virtual machine to shut down. If the virtual machine has not shut-down before the time-out period, the virtual machine forces a shutdown by the server.
Port	Sets the IP port number. This field is not available with VMware vSphere/ESX.

Converting BIOS vDisks to UEFI

This article explains how to convert the BIOS vDisks to UEFI. This conversion is important because BIOS support is removed in Citrix Provisioning™ version 2311 and onwards.

There are two approaches to convert an existing vDisk from BIOS format to UEFI:

- Convert the vDisk directly: Copy the `VHD(X)` file, mount it, convert, and then import the new file.
- Convert the vDisk using reverse imaging: Reverse image the vDisk to a master VM, reboot from the local disk, convert, and then create a new image.

> **Important:**
>
> In both the approaches, ensure that:
>
> - There is sufficient free space
> - The disk is defragmented before starting. You can do this step either after reverse imaging or before merging the vDisk to a single version.

> Image Portability Service can be used to automate the conversion to UEFI. For more information, see Convert to UEFI.

Convert the vDisk directly

Do the following steps to convert the vDisk directly:

1. Ensure that the disk is defragmented and merged down to a single base version.
2. Copy the `.VHD(X)` file to a new file in the store.
3. Run disk management in windows and attach the `VHD`.
4. Run `diskpart` to determine the disk number of the mounted disk.

```
C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer: JOEBL-PVS

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          127 GB  1024 KB        *
  Disk 1    Online          150 GB      0 B
  Disk 2    Online         1024 GB  1024 KB        *
  Disk 3    Online          127 GB  1024 KB        *
```

5. Run the following command to convert the mounted vdisk file to UEFI (GPT).

```
mbr2gpt /convert /disk:3 /allowFullOS
```

6. Unmount the `VHD` file and import into the Citrix Provisioning store.

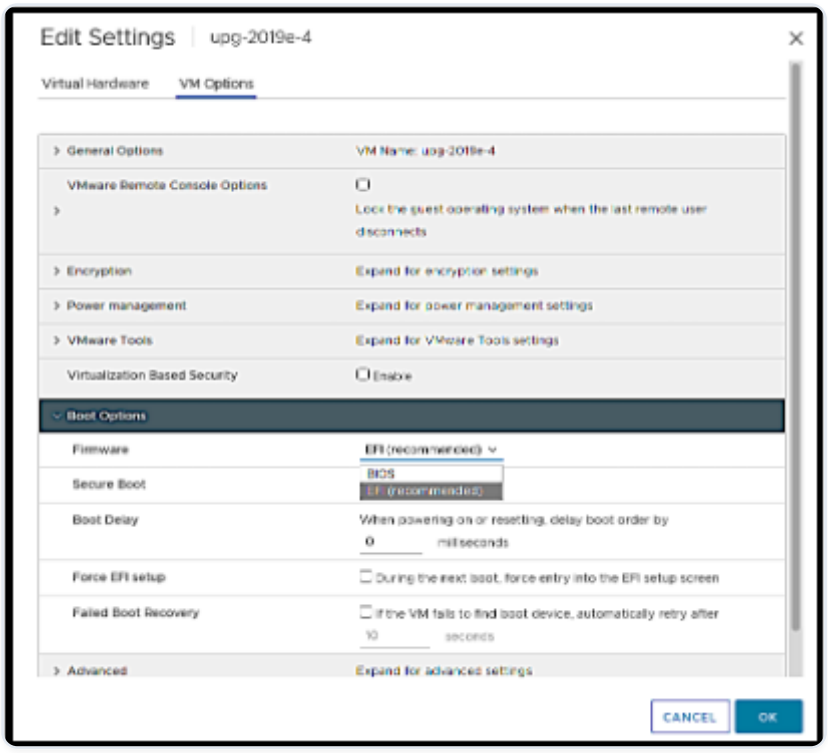
Convert the vDisk using reverse imaging

Do the following steps to Convert the vDisk using reverse imaging:

1. Reverse image to a master VM setup as BIOS with a local disk that is large enough.
2. Reboot the VM from the local disk (change the boot order) and log on as an administrator.
3. Run `diskpart` to confirm the disk number. The number must be zero.
4. Run the following command to convert the disk to UEFI (GPT).

```
mbr2gpt /convert /disk:0 /allowFullOS
```

5. Shut down the VM.
6. Update the hypervisor configuration for the VM to use UEFI. For example:
   - With VMware as a hypervisor, go to the VM **Edit Settings** and from the **VM Options tab> Boot Options** section, select the firmware type as **EFI**.



- With XenServer® as the hypervisor:

  a. Determine the UUID of the original VM. You can get the UUID from XenCenter® or use the `xe vm-list name-label="VM NAME"` as shown:

  ```
  [root@xenserver01 ~]# xe vm-list name-label="Windows 10 BIOS"

  uuid ( RO)           : e98a0a89-2fb9-886b-a843-b8a08642afa4

  name-label ( RW): Windows 10 BIOS

  power-state ( RO): halted
  ```

  b. Set the VM to use UEFI boot with `xe vm-param-set uuid=UUID HVM-boot-params:firmware=uefi` as shown:

  ```
  [root@xenserver01 ~]# xe vm-param-set uuid=e98a0a89-2fb9-886b-
  a843-b8a08642afa4 HVM-boot-params:firmware=uefi
  ```

7. Boot the VM and run the Imaging Wizard to create a new vDisk for the converted disk.

Retiring or deleting vDisks

A vDisk that is no longer needed can be retired by deleting it. All VHDX differencing disk files, properties files, lock files, and the difference cache are also deleted.

> **Note:**
>
> You cannot delete a vDisk if one or more target devices are currently assigned to it. Unassign all target devices from the vDisk, before attempting to delete it. When deleting a disk, a confirmation dialog appears indicating that you are removing the vDisk reference files in addition to the assigned device.

To delete a vDisk

1. In the Citrix Provisioning™ console, expand **vDisk Pool** in the tree, then highlight the vDisk that you want to delete in the details pane.
2. Right-click on the vDisk, then select **Delete**. The Delete vDisks dialog appears.
3. To delete the vDisk from the hard drive, select the check box for deleting the vDisk from the hard drive option. Or, do not select the check box to delete the vDisk from the store and database. The disk image file is permanently deleted unless a backup copy is made before deleting it from the store.
4. Click **Yes**. The vDisk is deleted.

Troubleshooting vDisks

vDisk not booting after promotion

PVS vDisk promotion is an explicit action you can perform as an IT administrator if you need to add updates or patches. This process starts in **Maintenance** mode. You can move (or promote) this new version to a **Test** or **Production** environment. In **Production**, all targets have access to this new PVS vDisk version for use during the next PVS vDisk boot.

There are three ways to promote PVS vDisks:

- **Maintenance** (read/write mode) to **Test** (read-only mode)
- **Maintenance** (read/write mode) to **Production** (read-only mode)
- **Test** to **Production** (read/write modes not applicable)

VHD-formatted PVS vDisks can become unbootable after promotion.

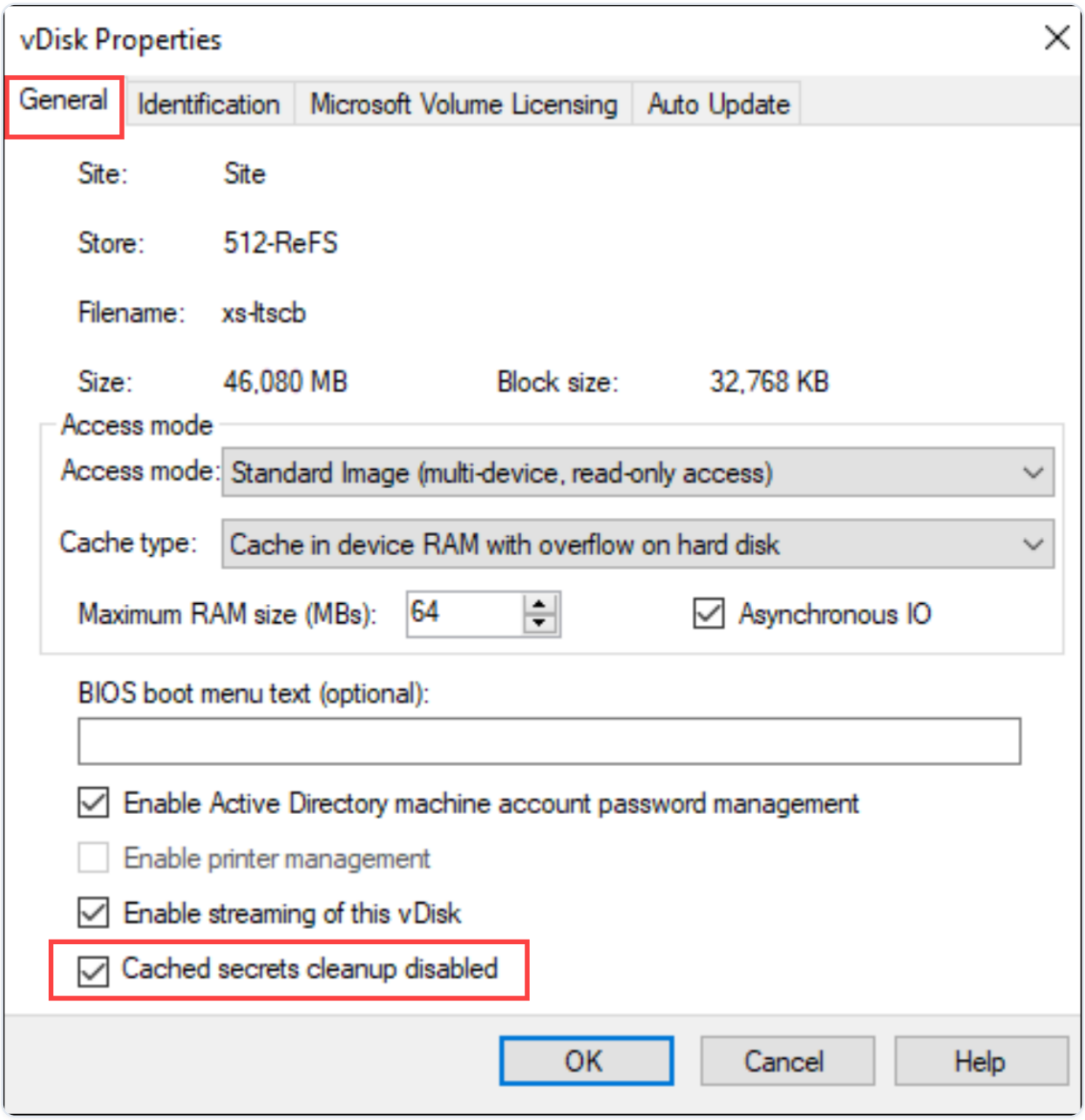
The content below provides troubleshooting steps you must perform if the PVS vDisk does not boot after promotion.

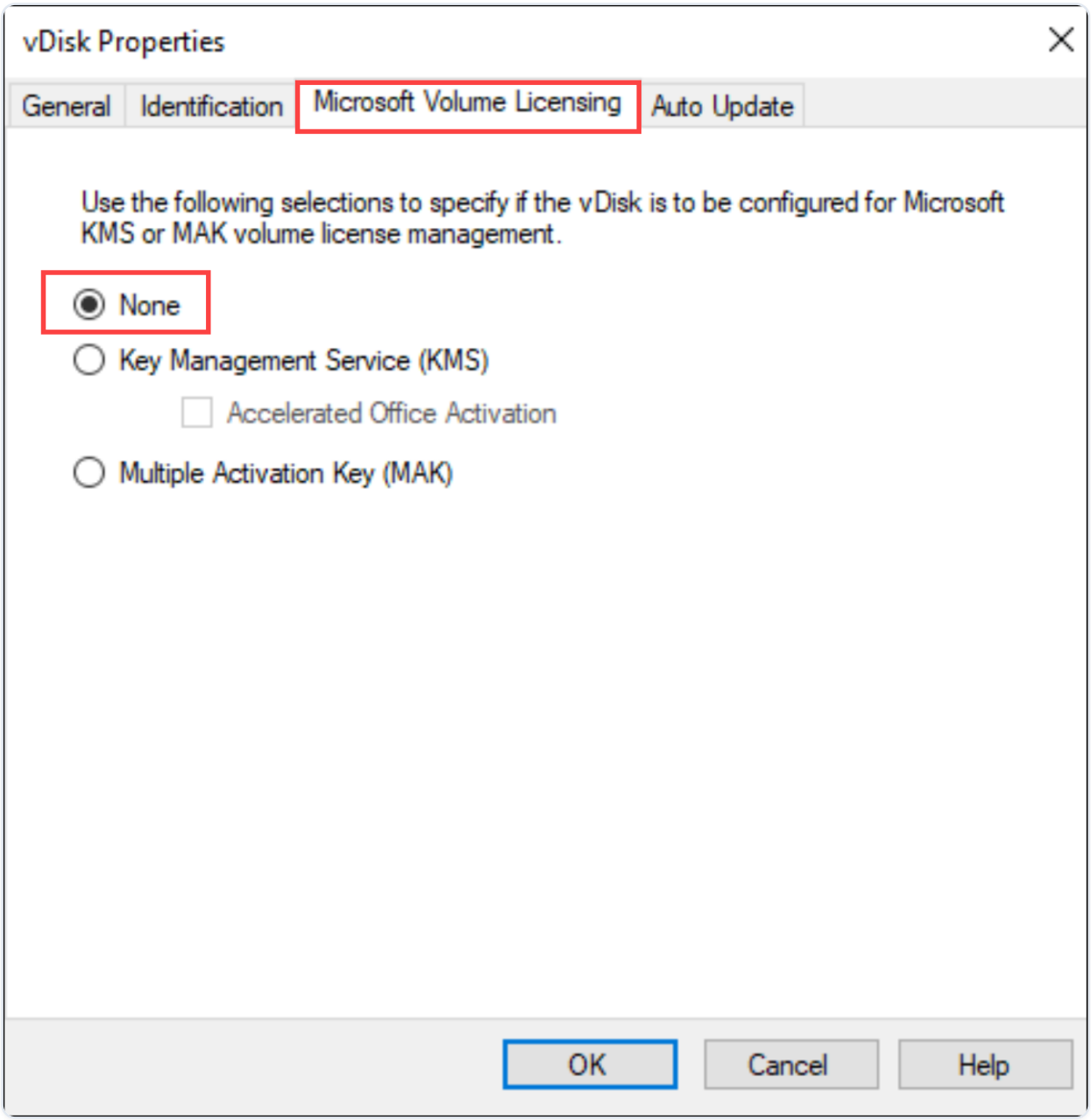
1. Create a problem report using the PVS console. You can save the report as a local .zip file.
2. Review the problem report with Support. Examining log messages is a critical step, enabling you to analyze and debug all events leading up to the boot failure.
3. Ensure you understand the PVS vDisk promotion process. If **Clean Cache Secrets** or **KMS Licensing** is enabled, the Provisioning server mounts the PVS vDisk locally to perform certain actions.

If the PVS vDisk uses a VHD format and does not boot after promotion, disable cache secret cleanup and KMS licensing support as follows:

1. Open the **vDisk Properties** window and, from the **General** tab, select the **Cached secrets cleanup disabled** checkbox. Alternatively, clearing the **Cached secrets cleanup disabled** checkbox enables the cleaning of cached secrets.
2. Select the **Microsoft Volume Licensing** tab and set **KMS** to **None**. You can select KMS licensing during PVS vDisk creation. You also can modify KMS licensing for an existing PVS vDisk version. The **General** and **Microsoft Volume Licensing** tabs allow you to make settings changes that can lead to PVS vDisk boot issues. For example, setting **KMS** to **None** can prevent the PVS server from modifying the PVS vDisk.

   Collectively, the **General** and **Microsoft Volume Licensing** tabs allow you to modify settings that – contingent upon your selections – can trigger the inability of VHD-formatted PVS vDisks to boot after promotion.


vDisk Properties
General
Identification
Microsoft Volume Licensing
Auto Update
Site: Site
Store: 512-ReFS
Filename: xs-ltscb
Size: 46,080 MB
Block size: 32,768 KB
Access mode
Access mode: Standard Image (multi-device, read-only access)
Cache type: Cache in device RAM with overflow on hard disk
Maximum RAM size (MBs): 64
Asynchronous IO
BIOS boot menu text (optional):
Enable Active Directory machine account password management
Enable printer management
Enable streaming of this vDisk
Cached secrets cleanup disabled
OK
Cancel
Help



3. Create a new version of the PVS vDisk and promote to **Test** or **Production**. Next, you must determine if the targets now use this PVS vDisk boot appropriately. To clarify, if you make these changes and the resulting PVS vDisk DOES boot, you have confirmed that you are encountering the bug associated with VHD-formatted PVS vDisks.
4. To resolve boot failure after PVS vDisk promotion, convert your VHD-based PVS vDisk to a .vhdx PVS vDisk format. For more information, see the Support Knowledge Center.

Views

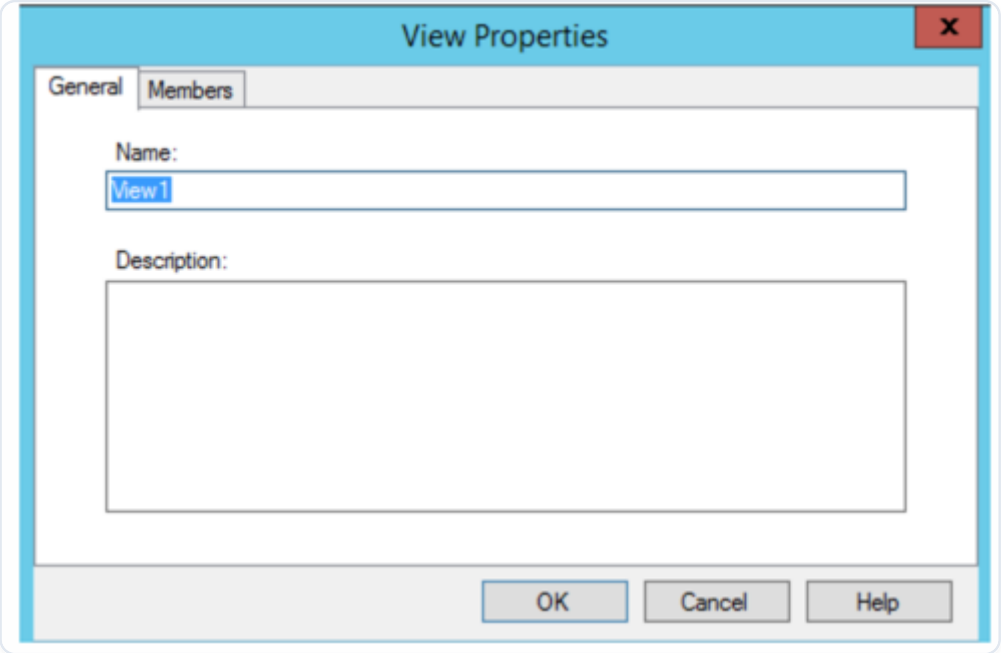
The Citrix Provisioning™ console view provides a method that allows you to quickly manage a group of devices. Views are typically created according to business needs. For example, a view

can represent a physical location, such as a building or user type. Unlike device collections, a target device can be a member of any number of views.

Farm administrators create and manage views in the console tree's **Farm > Views** folder. Farm views include any target device that exists in this farm. Site administrators can create and manage views in the console tree's **Farm > Sites > YourSite > Views** folder. Site views can only include target devices that exist within that site, *YourSite*.

View properties

To display or edit the properties of an existing view, right-click on the view in the console, then select the **Properties** menu option. The **View Properties** dialog displays.



View properties are described in the tables that follow.

General tab

FIELD	DESCRIPTION
Name	The name given to this view.
Description	Describes the purpose of this view.

Members tab

FIELD	DESCRIPTION
Member of this view	Lists target device members that belong to this view.
Add	Opens the **Select Devices** dialog, from which target devices to add to this view are selected.
Remove	Removes highlighted target devices from this view.
Remove all	Removes all target devices from this view.

Manage views in the Citrix Provisioning console

Use the information in this section to manage views.

Create a view

1. In the console, right-click on the **Views** folder where the new view exists, then select the **Create view** menu option. The **View Properties** dialog appears.
2. On the **General** tab, type a name for this new view in the **Name** text box. Optionally include a description, then click the **Members** tab.
3. Click the **Add** button to add new target device members to this view. The **Select Devices** dialog appears.
4. From the menus, select the site, then the device collection that you want to add target devices from. All members of that device collection appear in the list of available target devices.
5. Highlight one of more target devices in this collection, then click **Add** to add them to the new view. To add more target devices from other device collections, repeat steps 4 and 5.
6. Click **OK** to close the dialog. All selected target devices now display on the **Members** tab.

Paste device properties

To copy and paste device properties to members in a view:

1. In the console details pane, right-click on the target device that you want to copy properties from, then select **Copy device properties**. The **Copy Device Properties** dialog appears.

2. Select the check box next to the properties that you want to copy, then click **Copy**. The properties are copied to the clipboard and the dialog closes.
3. Right-click on the view containing the target devices that inherit the copied properties, then select the **Paste device properties** menu option. The **Paste Device Properties** dialog appears to display the name and properties of the target device that were copied.
4. Under the **Paste to table** heading, highlight the target devices that inherit these properties, then click **Paste**.
5. Click **Close**.

Delete a view

If a view becomes obsolete, you can delete the view. Deleting a view does not delete the target device from the collection.

1. In the console's tree, right-click on the view folder that you want to delete, then select the **Delete** menu option. A confirmation message appears.
2. Click **OK** to delete this view. The view no longer displays in the console tree.

Refresh a view

After modifying a view, refresh the view before those changes appear in the console. To refresh the view, right-click on the view in the tree, then select the **Refresh** menu option.

Start devices within a view

1. Right-click on the view in the console tree, then select the **Boot devices** menu option. The **Target Device Control** dialog displays with the Boot devices menu option selected in the **Settings** menu. By default, all devices are highlighted in the **Device** table.
2. Click the **Boot devices** button to boot target devices. The **Status** column displays the **Boot Signal status** until the target device boots. As each target device successfully boots, the status changes to **Success**.

Restart devices within a view

1. Right-click on the view in the console tree, then select the **Restart** devices menu option. The **Target Device Control** dialog displays with the **Restart devices** menu option selected in the **Settings** menu. By default, all devices are highlighted in the **Device** table.
2. Type the number of seconds to wait before restarting target devices in the **Delay** text box.
3. Type a message to display on target devices in the **Message** text box.

4. Click the **Restart devices** button to restart target devices. The **Status** column displays the **Restart Signal status** until the target device restarts. As each target device successfully restarts, the status changes to **Success**.

Shut down devices within a view

1. Right-click on the view in the console tree, then select the **Shutdown devices** menu option. The **Target Device Control** dialog displays with the **Shutdown devices** menu option selected in the **Settings** menu. By default, all devices are highlighted in the **Device** table.
2. Type the number of seconds to wait before shutting down target devices in the **Delay** text box.
3. Type a message to display on target devices in the **Message** text box.
4. Click the **Shutdown devices** button to shut down target devices. The **Status** column displays the **Shutdown Signal status** until the target device shuts down. As each target device successfully shuts down, the status changes to **Success**.

Send messages to target devices within a view

To send a message to target devices members within a view

1. Right-click on the view in the console tree, then select the **Send message menu** option. The **Target Device Control** dialog displays with the **Message to devices** menu option selected in the **Settings** menu. By default, all devices are highlighted in the **Device** table.
2. Type a message to display on target devices in the **Message** text box.
3. Click the **Send message** button. The **Status** column displays the **Message Signal** status until target devices receive the message. As each target device successfully receives the message, the status changes to **Success**.

Administrative roles

The administrative role assigned to a group of users controls viewing and managing objects within a Citrix Provisioning™ server implementation. Citrix Provisioning uses groups that exist within the network, Windows, or Active Directory Groups. All members within a group have the same administrative privileges within a farm. An administrator has multiple roles if they belong to more than one group.

The following administrative roles can be assigned to a group:

- Farm administrator
- Farm read-only administrator

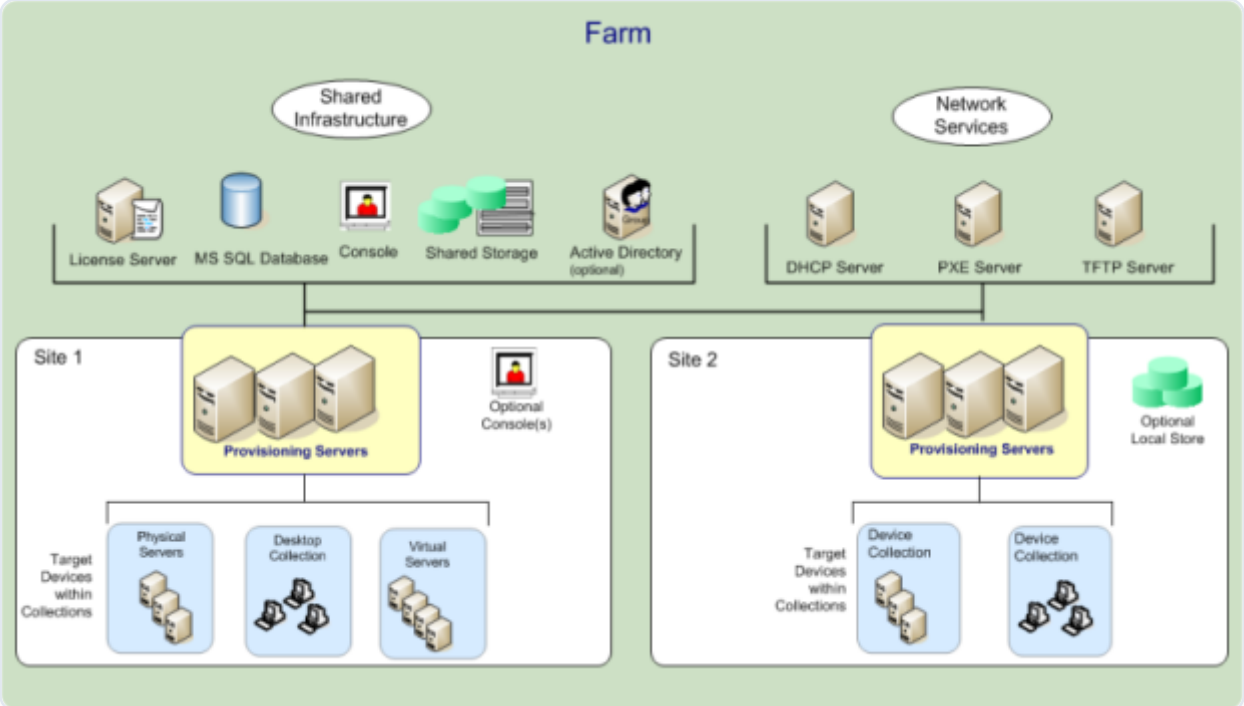
- Site administrator
- Device administrator
- Device operator

After a group is assigned an administrative role using the Citrix Provisioning console, certain requirements are required. If a member of that group attempts to connect to a different farm, a dialog displays requesting that you identify a provisioning server within that farm. Use either the Windows credentials you are currently logged in with, the default setting, or enter your Active Directory credentials. Citrix Provisioning does not support using both domain and workgroups simultaneously.

The role associated with the group determines your administrative privileges within this farm. Group role assignments can vary from farm to farm.

Managing farm administrators

Farm administrators view and manage all objects within a farm, and also create sites and manage role memberships throughout the entire farm. In the Citrix Provisioning console, administrators perform farm-level tasks.



When the farm is first configured using the Configuration Wizard, the administrator that creates the farm is automatically assigned the **Farm Administrator** role. While configuring the farm, that administrator selects the option to use either Windows or Active Directory credentials for user authorization within the farm. After an administrator runs the Configuration Wizard, more groups can be assigned the farm administrator role in the console.

To assign more farm administrators

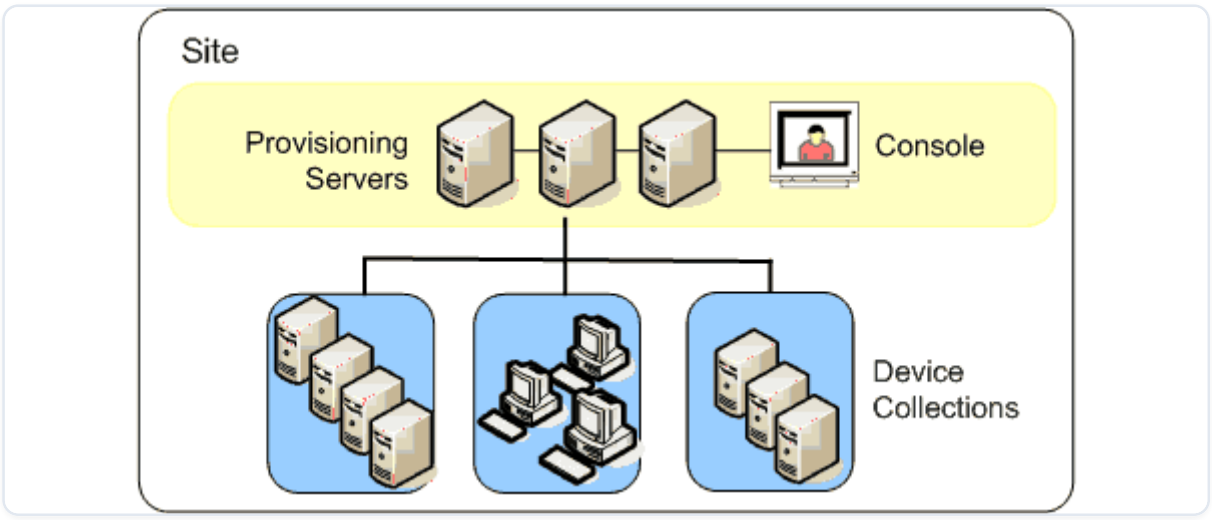
1. In the console, right-click on the farm to which the administrator role is assigned, then select **Properties**. The **Farm Properties** dialog appears.
2. On the **Groups** tab, highlight all the groups assigned administrative roles in this farm, then click **Add**. In the **Add Systems Group** dialog, add groups to give access rights. Click **OK**.
3. On the **Security** tab, select the groups to which you want to provide read-only access. The groups that are not selected will have read-write access. Click **Add** if you want to add groups to the list.
4. Click **OK** to close the dialog box.

Note:

The authorization method displays to indicate if Windows or Active Directory credentials are used for user authorization in this farm. The groups for administrative roles are limited to groups in the native domain and domains with a two-way trust to the native domain.

Managing site administrators

Site administrators have full management access to all the objects within a site. For example, the site administrator manages provisioning servers, site properties, target devices, device collections, virtual disk assignments pools.



If a farm administrator assigns a site as the owner of a particular store, the site administrator can also manage that store. Managing a store includes adding and removing virtual disks from shared storage or assigning provisioning servers to the store. The site administrator can also manage device administrator and device operator memberships.

To assign the site administrator role to one or more groups and its members

1. In the console, right-click on the site for which the administrator role is assigned, then select **Properties**. The **Site Properties** dialog appears.
2. Click the **Security** tab, then click the **Add** button. The **Add Security Group** dialog appears.
3. From the menu, select the groups to which you want to provide access.
4. Optionally, repeat steps 2 and 3 to continue assigning more site administrators.
5. Click **OK** to close the dialog.

Managing device administrators

Device administrators manage device collections to which they have privileges. Management tasks include assigning and removing a virtual disk from a device, editing device properties and viewing read-only virtual disk properties. Device collections consist of a logical grouping of devices. For example, a device collection might represent a physical location, a subnet range, or a logical grouping of target devices. A target device can only be a member of one device collection.

To assign the device administrator role to one or more groups and its members

1. In the console, expand the site where the device collection exists, then expand the **Device Collections** folder.
2. Right-click on the device collection that you want to add device administrators to, then select **Properties**. The **Device Collection Properties** dialog appears.
3. On the **Security** tab, under the **Groups with Device Administrator** access list, click **Add**. The **Add Security Group** dialog appears.
4. From the menu, select the groups to which you want to provide access.
5. Click **OK** to close the dialog box.

Managing device operators

A device operator has administrator privileges to perform the following tasks within a device collection for which they have privileges:

- Boot and reboot a target device
- Shut down a target device

To assign the device operator role to one or more groups

1. In the console, expand the site where the device collection exists, then expand the **Device Collections** folder.
2. Right-click on the device collection that you want to add device operators to, then select **Properties**. The **Device Collection Properties** dialog appears.
3. On the **Security** tab, under the Groups with **Device Operator access** list, click **Add**. The **Add Security Group** dialog appears.
4. To assign a group the **Device Operator** role, select each system group that requires device operator privileges, then click **OK**.
5. Click **OK** to close the dialog box.

Modifying the search approach for AD environments

For some AD environments containing configurations with complex nested groups and domains with many trust associations, the default method might be unable to find the user's expected administrative memberships. To resolve such scenarios, use a registry setting to change the search approach:

1. In the registry setting, locate `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices`.
2. Create a DWORD named "DomainSelectOption".
3. In the `DomainSelectOption DWORD`, set one of the following values (in decimal format) for the desired search approach:

- 0 – The default search. This method searches the user's domain followed by administrative group domains.
- 1 – Search in the user's domain and in the administrative group domain, followed by other trusted domains within a user's domain.
- 2 – Obsolete.
- 3 – Search in the user's domain followed by administrative group domains. The groups that are discovered are further enumerated over the parent's domain.
- 4 – Search the user's domain and in the administrative group domain, followed by other trusted domains within a user's domain. The groups that are discovered are further enumerated over the parent's domain.
- 5 - Search the user's group membership from token groups in the user's domain and in the administrative group domain.

- 6 - Search the user's group membership from token groups in the user’s domain and in the administrative group domain, followed by other trusted domains within a user’s domain.
- 7 - Search the user's group membership directly from authorization groups.
- 8 - Search the user's group membership directly as "Member Of" groups.

About whitelist methods

Use the information in this section for diagnostic purposes only. Sometimes, it may helpful to specify a specific domain for a user group to search against. To perform this task, update the registry and provide a JSON file for the white list domain. Use only the default search option. If you are providing a black list domain, it is excluded from the white list domains. No search occurs when the end list is empty.

In the registry:

1. Locate `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices`.
2. Create a DWORD entry **WhitelistOnly.** Set the value to **1** to enable white list search.

Advanced concepts

These articles offer a deeper dive into the Citrix Provisioning™ product documentation. Use the information in these articles to reduce deployment time through expert techniques. The articles cite the technical expert or experts who have authored the content.

Windows Secure Boot certificate expiration and CA updates

As documented by Microsoft at Windows Secure Boot certificate expiration and CA updates - Microsoft Support, the current certificates used for validating binaries when using Secure Boot are expiring in 2026 and have been replaced by new CA certificates which are used in the future to validate that binaries are properly signed. When booting a Citrix Provisioning target VDA, there are two different certificates that are used:

- The CA certificate which is used to validate the Citrix Provisioning network boot program as it is loaded. This has to be present in the UEFI firmware storage in order to boot a Citrix Provisioning VDA.
    - The existing certificate that is expiring is the **Microsoft UEFI CA 2011**. For the moment, this is the certificate used to sign the Citrix Provisioning network boot program and this continues to work after the CA certificate expires unless it is revoked.
    - The new certificate is the **Microsoft UEFI CA 2023**. At some point in 2026, Citrix Provisioning releases will contain Network Boot Programs signed by this certificate at which point they will only load if the hypervisor has been updated to include it.
- The CA certificate which is used to validate the Windows boot loader. When using Citrix Provisioning, the Windows boot loader is validated by the Citrix Provisioning Network Boot Program which has the CA certificate embedded. Currently, shipping versions of Citrix Provisioning only include the old CA certificate but there will be releases that include the new one as well - Citrix Provisioning will try both old and new certificate when loading the Windows Boot Loader.
    - The existing certificate that is expiring is **Microsoft Windows Production PCA 2011**.
    - The new certificate is the **Windows UEFI CA 2023**.

Important:

Even after your hypervisor is upgraded to a release that includes the new certificates, any existing VMs are not automatically updated to include this - the certificate information is stored in the UEFI NVRAM which is part of the VM.

Upgrading your environment

The process of upgrading the environment has three or four steps depending on the boot method used for Citrix Provisioning targets:

1. Upgrade the hypervisor being used to a version that includes the new certificates.
2. Update any existing VMs so that they have the updated certificates present in their NVRAM.
3. Upgrade Citrix Provisioning to a version that includes both certificates used to sign the Windows Boot Loader.
4. If using BDM or ISO boot, then update all the BDMdisk and ISO images.

Important:

- Do steps 1 and 2 now to prepare your environment for the shift.
- Windows has published documentation on how to mitigate CVE-2023-24932 by revoking the old Secure Boot certificates. This MUST NOT be done until you have completely updated your Citrix Provisioning setup as documented herein, including upgrading to a Citrix Provisioning version where the firmware is signed with the new certificate (this will be announced in the “What's new” section of the release where this is done - at that point, Citrix Provisioning will only work if the hypervisor and VMs have been updated). See How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932.
- When the old certificates are to be revoked, it is necessary to update the hypervisor hosts with that change and then update all existing VMs again to pick up the fact that the old certificates have been revoked. This implies that you must do steps 1 and 2 again.

The following table shows the results when the steps are done:

INSTALLED HYPERVISOR	INSTALLED CITRIX PROVISIONING	RESULTS
Old	Old (existing LTSR CUs, 2507 and earlier). NBP signed with old CA cert and has old Windows cert embedded.	Secure Boot will continue to work until a Windows update that is signed by the new Windows CA is applied to the vDisk. At that point Secure Boot will stop working.
	New, 2411, 2603, updated LTSR CUs. NBP still signed with old CA cert, with old and new Windows cert embedded.	Currently, we are shipping Citrix Provisioning NBP signed by the old key which will continue to work. Secure Boot fully supported.
	New, 2607 onwards, all LTSR CUs released after June 2026. NBP signed with new CA cert with old and new Windows cert embedded.	Secure Boot will stop working after updating to these releases.
New (includes old and new CA certs)	Old. NBP signed with old CA cert and has old Windows cert embedded.	Secure Boot will continue to work until a Windows update that is signed by the new Windows CA is applied to the vDisk. At that point Secure Boot will stop working.
	New, 2411, 2603, existing LTSR CUs. NBP still signed with old CA cert, with old and new Windows cert embedded.	Currently, we are shipping PVS NBP signed by the old key which will continue to work. Secure Boot fully supported.
	New, 2607 onwards (worst case), All LTSR CUs released after June 2026. NBP signed with new CA cert with old and new Windows cert embedded.	Secure Boot fully supported.

Upgrading the hypervisor

You should upgrade your hypervisor to a version that is at least what is outlined in the following table (note that earlier releases are not supported once the Secure Boot certificates are being used by Microsoft to sign binaries):

HYPERVISOR	MINIMUM VERSION
VMWare/ESXi	vSphere 8.0 update 3h
XenServer	8.4, November 2025 update
Hyper-V	Host should be running Server 2019 and newer with latest windows updates. Note that the process to enable the new certificates requires manual steps but Server 2022 and 2025 are automatically done as part of the windows update procedure. See Updating Server 2019 to enable the new CA certificates for details of enabling the new certificates in Server 2019 Hyper-V hosts.
Azure	The new certificates were available as of late 2024. Any VMs created before this time will have to be reprovisioned.
Nutanix	AVH 20230302.101026, associated with AOS 6.5.1
OpenShift	Version 4.17 or later
GCP	Google do not document when the new certificates were included. You should check any existing VMs using the script included later to see if the VMs already have the newer certificates present.

Upgrading existing VMs

Any VMs using Secure Boot that existed before the hypervisor was upgraded must be updated. The simplest and safest approach is to reprovision these VMs but most environments provide tools to help update existing VMs as documented in the following table:

Note:

If the VM also has a virtual TPM enabled, then it is not possible to update existing VMs and they must be reprovisioned.

HYPERVISOR	PROCEDURE
VMware vSphere 8	Not possible - you must reprovision all Citrix Provisioning target VMs.
VMware vSphere 9	You can reset a virtual machine's Secure Boot keys to the factory defaults (restoring the original trusted CA certificates, such as Microsoft UEFI CA and Microsoft Windows Production CA) using either the vSphere Client UI or the vicfg-uefi CLI tool.
XenServer 8.4	Not possible. You must reprovision all Citrix Provisioning target VMs.
Hyper-V	The Secure Boot certificates can be reset to the current set by toggling the Secure Boot Template to another value and then back to the MicrosoftUEFI Secure Boot template.
Other Hypervisors	Citrix Provisioning targets using Secure Boot must be reprovisioned.

If you are unsure how many Citrix Provisioning targets are using Secure Boot, see Determine if a VM uses secure boot and has the new certificates for instructions on checking this.

Determine if a VM uses Secure Boot and has the new certificates

You can determine if a VM is using Secure Boot by running `msinfo32` inside the VM but this won't tell you if the VM has the new certificates available or not.

See Appendix 1 for a script that be run from a Windows VM to determine if it is using Secure Boot and whether or not it has the new certificates.

See Appendix 2 for detailed information on updating existing VMs if you decide not to simply reprovision.

Upgrade the Citrix Provisioning target boot process

There are three boot methods for Citrix Provisioning targets, each of which require different work to enable the new certificates to be used:

- Network/PXE Boot: when the Citrix Provisioning farm is completely upgraded, targets that use PXE Boot automatically gets the updated Citrix Provisioning boot program the next time they boot.
- BDM Disk Boot: once the farm is completely upgraded, update all of the BDM disks for targets that use Secure Boot. The BDM update process that is available in the Citrix Provisioning console can be used for this. In addition, use the PowerShell cmdlet `Start-PvsDeviceUpdateBdm` to update individual devices or all devices in a collection
- ISO Boot: once the farm is completely updated, use the `BDM.exe` program to create new ISO images as required, upload to the hypervisor and change all VM definitions to boot from the updated ISO.

Appendix 1

The following script can be run in a Windows VM to determine if it uses Secure Boot and whether or not it already has the new certificates available.

Script: `Extract-db.ps1`

```
# dumpdb-fixed.ps1

$ErrorActionPreference = "Stop"



Write-Host "SecureBoot enabled:" (Confirm-SecureBootUEFI)



$db = Get-SecureBootUEFI -Name db

$bytes = $db.Bytes



$outDir = Join-Path $env:TEMP ("uefi-db-certs-" + (Get-Date -Format
"yyyyMMdd-HHmmss"))
```

```
New-Item -ItemType Directory -Path $outDir | Out-Null



$dbPath = Join-Path $outDir "db.bin"

[IO.File]::WriteAllBytes($dbPath, $bytes)

Write-Host "Wrote raw UEFI db to: $dbPath"

Write-Host "Parsing for X.509 certs..."



function Read-GuidFromBytes {

  param(

    [byte[]]$b,

    [int]$offset

  )

  if ($offset -lt 0 -or ($offset + 16) -gt $b.Length) {

    throw "GUID read out of range at offset $offset (len=$($b.Length))"

  }



  $gBytes = New-Object byte[] 16

  [Array]::Copy($b, $offset, $gBytes, 0, 16)



  # IMPORTANT: force the Guid(byte[]) ctor

  return [Guid]::new($gBytes)

}
```

```
$EFI_CERT_X509_GUID = [Guid]"a5c059a1-94e4-4aa7-87b5-ab155c2bf072"

$pos = 0
$certIndex = 0
$records = @()

while ($pos -lt $bytes.Length) {
  if ($pos + 28 -gt $bytes.Length) { break }

  $sigType  = Read-GuidFromBytes -b $bytes -offset $pos
  $listSize = [BitConverter]::ToUInt32($bytes, $pos + 16)
  $hdrSize  = [BitConverter]::ToUInt32($bytes, $pos + 20)
  $sigSize  = [BitConverter]::ToUInt32($bytes, $pos + 24)

  # sanity checks
  if ($listSize -lt 28) { break }
  if ($sigSize -lt 16)  { break }
  if (($pos + $listSize) -gt $bytes.Length) { break }

  $sigDataStart = $pos + 28 + $hdrSize
  $sigDataEnd   = $pos + $listSize
```

```
  if ($sigDataStart -gt $sigDataEnd) { break }


  $entryCount = [Math]::Floor( ($sigDataEnd - $sigDataStart) / $sigSize )


  for ($i = 0; $i -lt $entryCount; $i++) {
    $entryOffset = $sigDataStart + ($i * $sigSize)


    if ($entryOffset + $sigSize -gt $bytes.Length) { continue }


    $owner = Read-GuidFromBytes -b $bytes -offset $entryOffset
    $dataOffset = $entryOffset + 16
    $dataLen    = $sigSize - 16


    if ($sigType -eq $EFI_CERT_X509_GUID) {
      $certBytes = New-Object byte[] $dataLen
      [Array]::Copy($bytes, $dataOffset, $certBytes, 0, $dataLen)


      try {
        $cert =
[System.Security.Cryptography.X509Certificates.X509Certificate2]::new($cer
tBytes)


        $certIndex++
```

```
        $cerPath = Join-Path $outDir ("db-cert-{0:D3}.cer" -f $certIndex)
        [IO.File]::WriteAllBytes($cerPath, $certBytes)

        $records += [PSCustomObject]@{
          Index      = $certIndex
          OwnerGuid  = $owner.ToString()
          Subject    = $cert.Subject
          Issuer     = $cert.Issuer
          Thumbprint = $cert.Thumbprint
          NotBefore  = $cert.NotBefore
          NotAfter   = $cert.NotAfter
          Path       = $cerPath
        }
      } catch {
        # ignore non-parseable entries
      }
    }
  }

  $pos += $listSize
}
```

```
$csvPath = Join-Path $outDir "db-certs.csv"

$records | Export-Csv -NoTypeInformation -Path $csvPath



Write-Host ""

Write-Host "Extracted $($records.Count) X.509 cert(s) from UEFI db."

Write-Host "Output directory: $outDir"

Write-Host "CSV summary:      $csvPath"

$records | Select-Object Index, Thumbprint, NotAfter, Subject | Format-
Table -AutoSize
```

Sample output for a VM that does not have the new certificates.

```
PS C:\Users\simong\Downloads> .\Extract-db.ps1

SecureBoot enabled: True

Wrote raw UEFI db to: C:\Users\simong\AppData\Local\Temp\uefi-db-
certs-20260305-131219\db.bin

Parsing for X.509 certs...



Extracted 2 X.509 cert(s) from UEFI db.

Output directory: C:\Users\simong\AppData\Local\Temp\uefi-db-
certs-20260305-131219

CSV summary:      C:\Users\simong\AppData\Local\Temp\uefi-db-
certs-20260305-131219\db-certs.csv



Index Thumbprint                                NotAfter
 Subject
```

```
----- ----------                                  --------
 -------

    1 580A6F4CC4E4B669B9EBDC1B2B3E087B80D0678D 10/19/2026 2:51:42 PM
CN=Microsoft Windows Production PCA 2011, O=Mic...

    2 46DEF63B5CE61CF8BA0DE2E6639C1019D0ED14F3 6/27/2026 5:32:45 PM
 CN=Microsoft Corporation UEFI CA 2011, O=Micros...
```

VMware

Using PowerCLI (Recommended)

1. Install or import PowerCLI.

   ```
   Install-Module -Name VMware.PowerCLI -Scope CurrentUser

   Import-Module VMware.PowerCLI
   ```

2. Connect to your vCenter or ESXi host.

   ```
   Connect-VIServer -Server <your-vcenter-or-esxi-host>
   ```

3. Check Secure Boot for:

   - All VMs:

     ```
     Get-VM | Select Name, @{N='SecureBoot';E={ ($_ | Get-
     VMFirmware).EnableSecureBoot }}
     ```

   - A specific VM:

     ```
     $vm = Get-VM -Name 'YourVMName'

     $firmware = $vm | Get-VMFirmware

     $firmware.EnableSecureBoot   # Returns True or False
     ```

   Output:

- `True`: Secure Boot is enabled.
- `False`: Secure Boot is disabled.

Query via PowerCLI Script

```
# List all VMs and their Secure Boot state

Get-VM | Select-Object Name, @{N='SecureBootEnabled';
E={$_.ExtensionData.Config.BootOptions.EfiSecureBootEnabled}}
```

Using the vSphere API (Python example)

With pyVmomi, you can programmatically access the same value:

```
from pyVim.connect import SmartConnect, Disconnect

from pyVmomi import vim

# (login and setup code here...)

vm = # get your VM object

if vm.config.firmware == "efi":

    print(f"Secure Boot enabled:
{vm.config.bootOptions.efiSecureBootEnabled}")

else:

    print("VM does not use EFI firmware.")
```

Summary table

METHOD	SCRIPT/COMMAND	OUTPUT
PowerCLI	`Get-VMFirmware` and `EnableSecureBoot`	True/False per VM
pyVmomi (Python)	`vm.config.bootOptions.efiSecureBootEnabled`	True/False

XenServer

To test whether a VM uses Secure Boot in XenServer 8.4, you need to check the VM's configuration for the secure_boot parameter in the VM's platform settings. Perform the following steps in the built-in xe CLI, which is the most straightforward and scriptable method.

1. List Your VMs.

   ```
   xe vm-list is-control-domain=false
   ```

   Find your VM's uuid.

2. Inspect platform parameters for Secure Boot.

   ```
   xe vm-param-get uuid=<VM-UUID> param-name=platform
   ```

   Sample output:

   Not `secureboot: true` in the following:

   ```
   [root@ra-xen-04 ~]# xe vm-param-get uuid=740a8d85-c096-c9cd-
   b83e-2c106513415f param-name=platform

   timeoffset: -18002; device-model: qemu-upstream-uefi; cores-per-socket:
   2;

   device_id: 0002; viridian: true; viridian_time_ref_count: true;

   viridian_reference_tsc: true; viridian_apic_assist: true;
   viridian_crash_ctl: true;

   viridian_stimer: true; secureboot: true; vga: std; videoram: 8; nx:
   true;

   acpi: 1; apic: true; pae: true; hpet: true; acpi_laptop_slate: 1; vtpm:
   true
   ```

   Interpretation:

   - If you see `secure_boot: true`, then the VM is using Secure Boot.
   - If you see `secure_boot: false` or the key is missing, Secure Boot is not enabled.

3. Script to Check all VMs. The following is a bash snippet to list all VMs and their Secure Boot status.

```
for UUID in $(xe vm-list is-control-domain=false --minimal | tr ','
'\n'); do

NAME=$(xe vm-param-get uuid=$UUID param-name=name-label)

PLATFORM=$(xe vm-param-get uuid=$UUID param-name=platform)

SECURE_BOOT=$(echo "$PLATFORM" | grep -oE 'secureboot: [^;]+' | awk
'{print $2}')

echo "$NAME: Secure Boot = ${SECURE_BOOT:-not set}"

done
```

You can also print the names of all VMs that are using secure Boot:

```
xe vm-list platform:secureboot=true params=name-label --minimal|tr ','
'\n'

ra-w11-cvad002

ra-w11-cvad027

ra2-w11-cvad029

ra-w11-cvad029

ra2-w11-cvad020

ra-w11-cvad014

ra-w11-cvad020

ra-w11-cvad016

ra-w11-cvad003

...
```

Summary table

PLATFORM PARAMETER	SECURE BOOT STATE
`secureboot: true`	Secure Boot is ON
`secureboot: false`	Secure Boot is OFF
`No secureboot key`	Secure Boot is not set/not supported

Checking templates

Any templates other than the built-in ones must be updated or recreated to ensure the updated certificates are present. The built-in template objects have `is-default-template=true` set so use the following command:

```
xe template-list params=name-label,is-default-template
```

Hyper-V

To check whether a Hyper-V VM has Secure Boot enabled, you can use PowerShell, which is scriptable and works locally or remotely.

> **Note:**
>
> The following commands must be run on the hyper-v host and not the machine with SCVMM installed.

1. List Secure Boot Status for all VMs.

   ```
   Get-VM | Get-VMFirmware -ErrorAction SilentlyContinue | Select-Object
   VMName, SecureBoot
   ```

   Sample output:

   ```
   PS C:\Users\administrator.CELESTIALS> Get-VM | Get-VMFirmware
   -ErrorAction SilentlyContinue | Select-Object VMName, SecureBoot
   ```

```
VMName     SecureBoot

------     ----------

2016                On

2025               Off

025-1             Off

simgr-2025          On
```

2. Check Secure Boot for one VM.

```
Get-VM -Name "YourVMName" | Get-VMFirmware | Select-Object SecureBoot
```

The property `SecureBootEnabled` is:

- `On` if Secure Boot is enabled.
- `Off` if Secure Boot is disabled.

Important:

Generation 2 VMs only: Secure Boot is only supported for Generation 2 VMs, which use UEFI firmware. Generation 1 (BIOS) VMs does not have this property.

Appendix 2

As previously stated, the safest approach is to reprovision all VMs that use Secure Boot but if this is not possible then this section describes how existing target VMs can be updated for those hypervisors that support updating.

VMware vSphere 9

In VMware vSphere 9, you can reset a virtual machine's Secure Boot keys to the factory defaults (restoring the original trusted CA certificates, such as Microsoft UEFI CA and Microsoft Windows Production CA) using the `vicfg-uefi CLI` tool.

CLI/PowerCLI method

Prerequisites:

- vSphere 9
- The VM must be powered off.

Commands

The basic requirement is to set the following advanced parameters for each VM to `TRUE`. These causes the VM to reload the certificates on next boot.

```
"uefi.secureBoot.PK.resetOnce"

"uefi.secureBoot.KEK.resetOnce"

"uefi.secureBoot.db.resetOnce"

"uefi.secureBoot.dbx.resetOnce"
```

The following script (`VMWare-ResetCertificates.ps1`) is an example of doing this for a specific VM (including connecting to the vCenter and setting parameters) to allow self-signed certificates to be used by the vCenter.

```
param (

    [Parameter(Mandatory=$true)]

    [string]$vCenter,



    [Parameter(Mandatory=$true)]

    [PSCredential]$Credential,



    [Parameter(Mandatory=$true)]

    [string]$VMName

)
```

```
# 1. Suppress CEIP warning and ignore invalid certificates for this
session only

Set-PowerCLIConfiguration -ParticipateInCEIP $false
-InvalidCertificateAction Ignore -Confirm:$false -Scope Session | Out-Null



# 2. Connect to vCenter

Write-Host "Connecting to vCenter: $vCenter..." -ForegroundColor Cyan

try {

    Connect-VIServer -Server $vCenter -Credential $Credential -ErrorAction
Stop

}

catch {

    Write-Error "Failed to connect to vCenter: $_"

    return

}



# 3. Get VM Object

$vm = Get-VM -Name $VMName -ErrorAction SilentlyContinue

if (-not $vm) {

    Write-Error "VM '$VMName' not found."

    Disconnect-VIServer -Server $vCenter -Confirm:$false

    return
```

```
}



# 4. Fail if the VM is not powered off

if ($vm.PowerState -ne "PoweredOff") {

    Write-Error "VM '$VMName' must be Powered Off to reset Secure Boot.
Current state: $($vm.PowerState)"

    Disconnect-VIServer -Server $vCenter -Confirm:$false

    return

}



# 5. Build and Apply Reset Spec

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec

$resetKeys = @(

    "uefi.secureBoot.PK.resetOnce",

    "uefi.secureBoot.KEK.resetOnce",

    "uefi.secureBoot.db.resetOnce",

    "uefi.secureBoot.dbx.resetOnce"

)



foreach ($key in $resetKeys) {

    $option = New-Object VMware.Vim.OptionValue

    $option.Key = $key
```

```
    $option.Value = "TRUE"

    $spec.ExtraConfig += $option

}



Write-Host "Applying Secure Boot reset flags to $VMName..."
-ForegroundColor Cyan

try {

    $vm.ExtensionData.ReconfigVM($spec)

    Write-Host "Success! Certificates will reset on the next power-on."
-ForegroundColor Green

}

catch {

    Write-Error "Failed to update configuration: $_"

}



# 6. Disconnect

Disconnect-VIServer -Server $vCenter -Confirm:$false
```

Hyper-V

In Hyper-V Gen 2 VMs, you can use PowerShell to change the Secure Boot template, which in practice resets the Secure Boot keys to the chosen "factory" set (either the Microsoft Windows Production CA or Microsoft UEFI CA).

This is the closest PowerShell-equivalent to a "reset to factory" for Secure Boot keys in Hyper-V.

How Secure Boot template works in Hyper-V

- Secure Boot Template = firmware's “preset” CA certificate selection.

- There are two built-in templates:
  - `MicrosoftWindows`: Only trusts the Microsoft Windows Production CA (good for all Windows OS).
  - `MicrosoftUEFICertificateAuthority`: Trusts the Microsoft UEFI CA (needed for most modern Linux distros with shim). This template MUST be selected for Citrix Provisioning streamed VMs.

Changing the template replaces the UEFI Secure Boot PK/KEK/db with the default set for that template. This effectively resets any custom or previously-enrolled keys back to the chosen set.

PowerShell instructions

> **Note:**
>
> This cannot be done if the VM has a vTPM.

1. List available Secure Boot templates.

```
(Get-VMHost).SecureBootTemplates



Id                                   Name
 Description

--                                   ----
 -----------

1734c6e8-3154-4dda-ba5f-a874cc483422 MicrosoftWindows
 Microsoft Windows

272e7447-90a4-4563-a4b9-8e4ab00526ce MicrosoftUEFICertificateAuthority
Microsoft UEFI Certificate Authority

4292ae2b-ee2c-42b5-a969-dd8f8689f6f3 OpenSourceShieldedVM
 Open Source Shielded VM
```

2. Look up VMs using the UEFI Secure Boot template. Use the following script.

```
Get-VM | Where-Object Generation -eq 2 | ForEach-Object {

$firmware = Get-VMFirmware -VM $_



if ($firmware.SecureBootTemplate -eq
"MicrosoftUEFICertificateAuthority") {

    [PSCustomObject]@{

        VMName     = $_.Name

        TPMEnabled = (Get-VMSecurity -VM $_).TPMEnabled

    }

}

} | Format-Table -AutoSize
```

Output:

```
PS C:\Users\administrator.CELESTIALS\Downloads> .\Get-PVSTargetVMs.ps1



VMName         TPMEnabled

------         ----------

mo-PVS13804-02       True

pvs-hv2022-1         True

pvs-hv2022-2         True
```

Note:

Remember that you cannot update VMs using a TPM. These have to be reprovisioned.

3. Change Citrix Provisioning targets using the UEFI template to Windows and then back to UEFI to reload the certificates.

```
# Set template to Windows CA only

Set-VMFirmware -VMName "YourVMName" -SecureBootTemplate
MicrosoftWindows

# Set template to Windows and UEFI CA

Set-VMFirmware -VMName "YourVMName" -SecureBootTemplate
MicrosoftUEFICertificateAuthority
```

- The new template overwrites any user-enrolled keys and bring the firmware back to the template's factory keys.
- VM must be powered off to change the template.

The following script (`Update-PVS-VMs.ps1`) changes all Citrix Provisioning VMs that are powered off that are not using a TPM.

```
# Get all VMs using the Microsoft UEFI CA template

$vms = Get-VM | Get-VMFirmware -ErrorAction SilentlyContinue| Where-
Object { $_.SecureBootTemplate -eq
"MicrosoftUEFICertificateAuthority" }



foreach ($vmFirmware in $vms) {

$vmName = $vmFirmware.VMName

$vm = Get-VM -Name $vmName



# Check for TPM status

$tpmStatus = (Get-VMSecurity -VMName $vmName).TpmEnabled
```

```
if ($tpmStatus -eq $true) {

    Write-Host "Ignoring VM: $vmName which has TPM enabled."
-ForegroundColor Red

    continue # Skip to the next VM in the loop

}



# Ensure VM is Off

if ($vm.State -ne 'Off') {

    Write-Host "Ignoring VM: $vmName which is on." -ForegroundColor Red

    continue

}



# Perform the toggle

Set-VMFirmware -VMName $vmName -SecureBootTemplate "MicrosoftWindows"

Set-VMFirmware -VMName $vmName -SecureBootTemplate
"MicrosoftUEFICertificateAuthority"



Write-Host "Processed VM: $vmName." -ForegroundColor Green

}
```

```
PS C:\Users\administrator.CELESTIALS\Downloads> .\Update-PVS-VMs.ps1

Ignoring VM: mo-PVS13804-02 which has TPM enabled.
```

```
Processed VM: simgr-sb.
```

Summary

Toggling the Secure Boot template in Hyper-V Gen 2 VMs through PowerShell is a supported way to reset the Secure Boot keys to the factory defaults for that template. This replaces the UEFI key store with the template's pre-set trusted certificates, removing any previous customizations.

Updating Server 2019 to enable the new CA certificates

Windows Server 2019 is fully supported for the new 2023 Secure Boot certificates, but because it is an older OS, the update behavior is more conservative compared to Windows 11. While the certificates are included in the monthly Cumulative Updates for Server 2019 (specifically those released from May 2024 onwards), they are often not applied automatically to avoid potential boot issues on older hardware or virtual environments.

- The "Support Status" for Server 2019 Physical servers running 2019 can receive the update, provided the server's BIOS/firmware is modern enough to handle the 2023 CA.

  However, note that unlike Windows 11, which might "auto-update" once Microsoft gains "high confidence" in the hardware, Server 2019 typically requires an administrator-initiated trigger through the registry.

Trigger the update on Server 2019

If you have confirmed your Server 2019 VM is fully patched but the certificates are still the 2011 versions, you can manually trigger the deployment using the following steps:

1. Set the Trigger Key: Open an elevated Command Prompt or PowerShell and run:

   ```
   reg add
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Secureboot /v
   AvailableUpdates /t REG_DWORD /d 0x5944 /f
   ```

   The value 0x5944 tells Windows to deploy all new 2023 CAs and the new signed Boot Manager.

2. Run the Scheduled Task: Windows uses a specific background task to process these certificate changes. You can start it immediately:

```
Start-ScheduledTask -TaskName "\Microsoft\Windows\PI\Secure-Boot-
Update"
```

3. Reboot: A restart is usually required for the Windows Boot Manager to switch to the version signed by the "Windows UEFI CA 2023."
4. Verification: After the reboot, run this PowerShell command to see if the 2023 CA is now in the allowed database (db):

```
[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes)
-match 'Windows UEFI CA 2023'
```

   - Returns True: You are protected and ready for the 2026 deadline.
   - Returns False: The update failed. This is common in Hyper-V if the VM's "Secure Boot Template" is set incorrectly.

Enable secure connection by limiting SQL server to TLS 1.2

Use the information in this section to modify secure connection from the provisioning server to the SQL server to limit it to TLS 1.2. For information on how to configure secure connecion from provisioning server to SQL server, see Enable secure connection from provisioning server to SQL server.

> **Note:**
>
> This implementation is applicable to only the SQL server Database.
>
> To use only TLS 1.2, disable all earlier versions of TLS. The following are the **Windows server** setting in the registry.

- `HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server Enabled = 0x00000000`
- `HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server Enabled = 0x00000000`

To disable the earlier versions of TLS, do the following on the SQL server computer:

1. Create **TLS 1.0** and **TLS 1.1** keys if they are not present under `SecurityProvider\SCHANNEL\Protocols`.
2. Create the server key under each one if it is not present.
3. Create the Enabled DWORD value under each one if it is not present.
4. Set the Enabled value to 0x00000000 (false).
5. Restart the Windows server.

For more information, see TLS registry settings.

Enable SQL Server Always On multi-subnet failover

Citrix Provisioning™ supports SQL Server Always On failover in multi-subnet environments. The Citrix Provisioning server requires Microsoft OLE DB Driver for SQL Server. Microsoft OLE DB Driver fully supports Always On availability groups.

Ensure that the provisioning server is configured to use the Always On availability group listener as the database server name. You do not need to use any instance name. When you use the availability group listener, enable **multiSubnetFailover**.

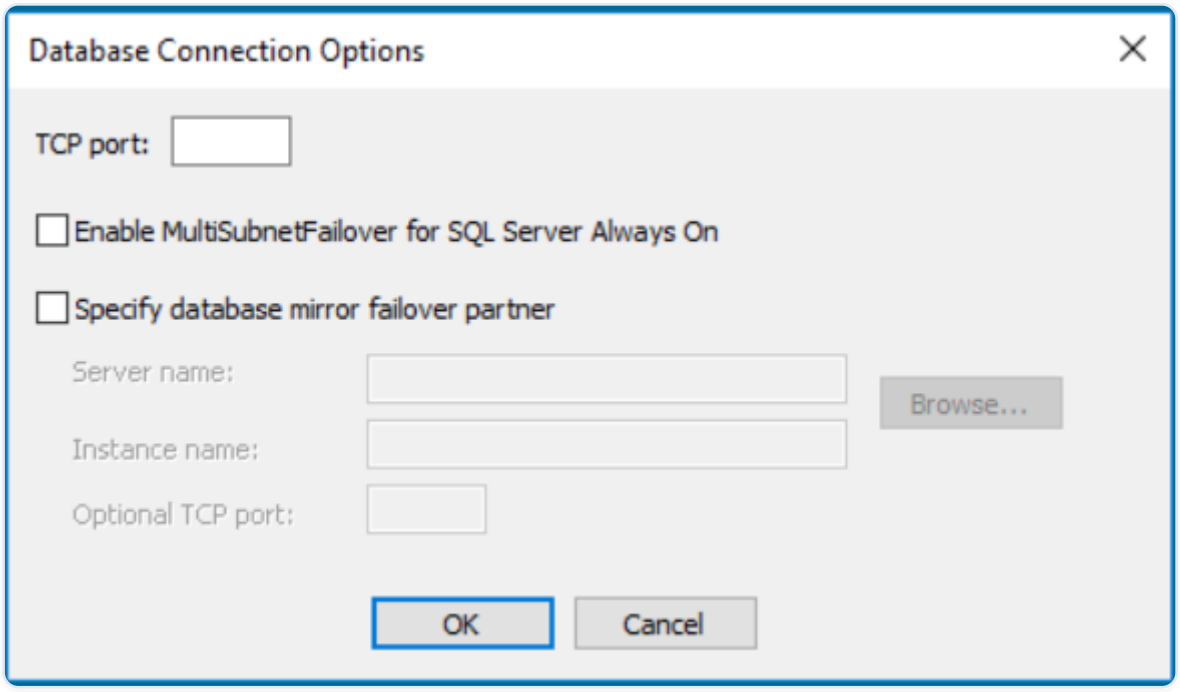
> **Tip:**
>
> The Microsoft OLE DB Driver is part of the Citrix Provisioning installer. No additional installation procedures are necessary to use this functionality.

> Enable always on failover using the **Enable MultiSubnetFailover for SQL** field on the **Database Connection Options dialog** in the Citrix Provisioning Configuration Wizard. To avoid potential configuration conflicts with other Citrix Virtual Apps and Desktops™ components, use only the configuration wizard to enable this feature.

> **Note:**
>
> For more information, see SQL Always On for SQL Server 2012, 2014, 2016 and 2017.

To enable SQL server always on in multi-subnet environments

1. After launching the Citrix Provisioning Configuration Wizard, access the **Database Server** screen.
2. On the **Database Server** screen:
    a. Click **Browse** to browse for existing SQL databases and instances in the network, or type the database server name and instance.
    b. Select **Active Directory Integrated** authentication if you want to use the services' user account. Enter the database credentials that the Stream and SOAP services will use.
    c. Click **Connections Options...**
3. On the **Database Connection Options** screen, select the **Enable MultiSubnetFailover for SQL Server Always On** check box.
4. On the **Database Server** screen, click **Next**.
5. Enter database administrator credentials in the pop-up dialog. Select **Active Directory Integrated** authentication if you want to use the current login. Click **OK**.
6. Complete the remaining wizard pages.



SQL basic availability groups

A basic availability group supports a failover environment containing a single database. SQL basic availability groups are configured the same way as SQL Always-On High Availability groups, with the following differences:

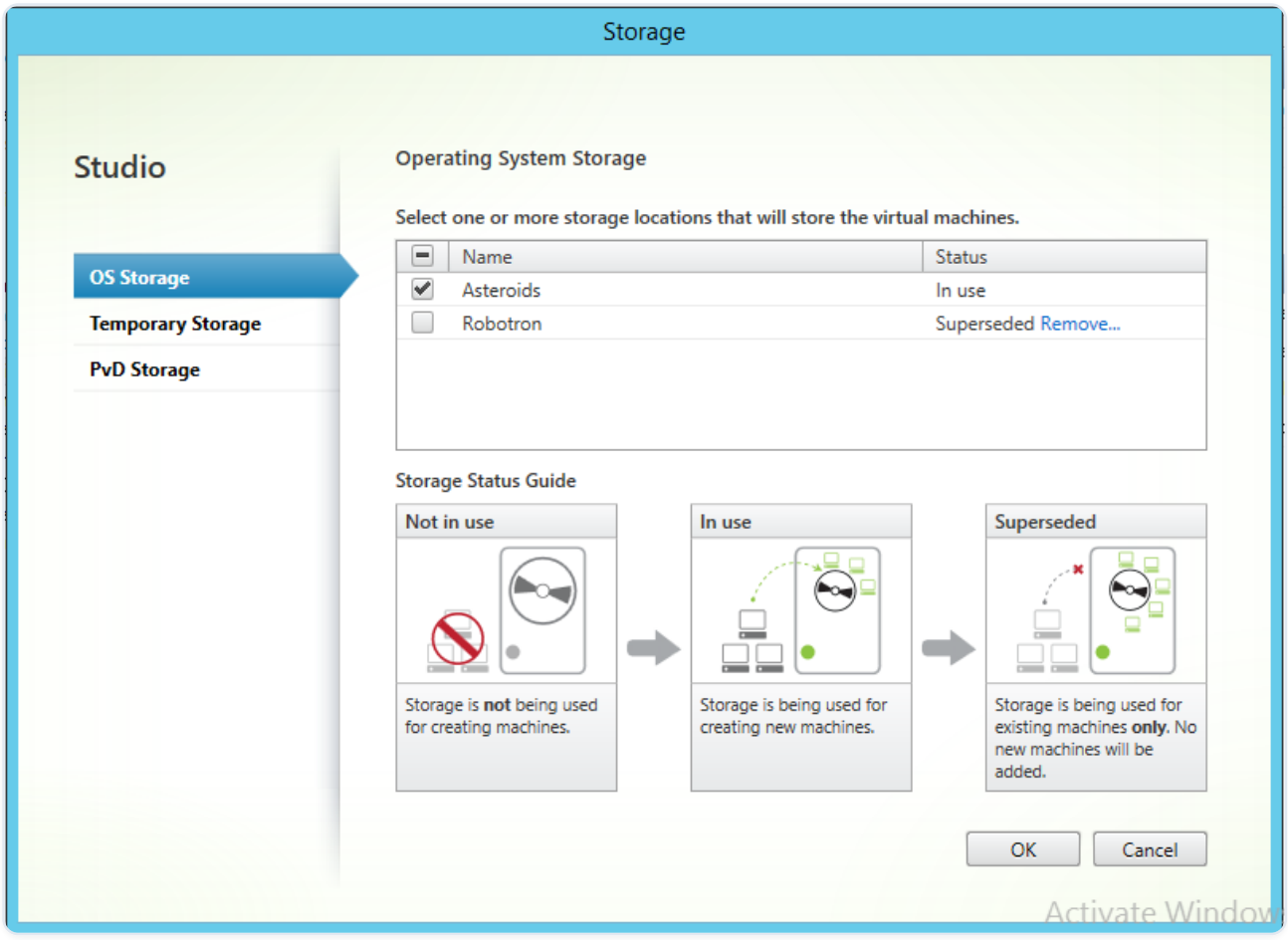
- Limit of two replicas (primary and secondary).
- No read access on secondary replica.
- No backups on secondary replica.
- No integrity checks on secondary replicas.
- Support for one availability database.
- Basic availability groups cannot be upgraded to advanced availability groups. The group must be dropped and readded to a group that contains servers running only SQL Server 2016 Enterprise Edition.
- Basic availability groups are only supported for Standard Edition servers.
- Basic availability groups cannot be part of a distributed availability group.

> **Tip:**
>
> For multi-subnet environments, see Enable SQL Always On multi-subnet failover.

Storage migration within the same host

Citrix Provisioning™ improves storage migration within the same host by updating how Citrix Studio integrates OS storage within a VM. To use this functionality:

1. In Citrix Studio, set the delivery group, containing members the desired target devices, to **maintenance mode**.
2. Shut down all provisioned target devices.
3. Go to **Configuration > Hosting** and select the **Host resource** that you want to change. In **Actions** portion of the screen, click **Edit Storage**.
4. In OS and temporary storages, clear the old storage. Changing the storage places the storage into **Superseded** status. Click **Remove...** to permanently remove it. Select the new storage you are going to use.



1. Go to the hypervisor and migrate the VMs to the new storage. Some hypervisors (ESX and VMM) have meta data for VMs. Move them also.
2. Disable maintenance mode on the delivery group.
3. Boot all the provisioned target devices.

Managing for highly available implementations

Establishing a highly available network involves identifying critical components, creating redundancy for these components, and ensuring automatic failover to the secondary component if the active component fails. Critical components include:

- Database
- Provisioning servers
- vDisks and storage

Citrix Provisioning™ provides several options to consider when configuring for a highly available implementation, including:

- Database

    - Offline database support, which allows Citrix Provisioning servers to use a snapshot of the database if the connection to the database is lost.
    - Database mirroring.

- Citrix Provisioning servers
    - Provisioning server failover. If a server becomes unavailable, another server within the site can provide active target devices with the virtual disk.
    - Managing servers. You can load balance between provisioning servers to prevent overload and to allow server capacity to be used more effectively and efficiently.

- vDisks and Storage
    - Configuring highly available shared storage

Offline database support

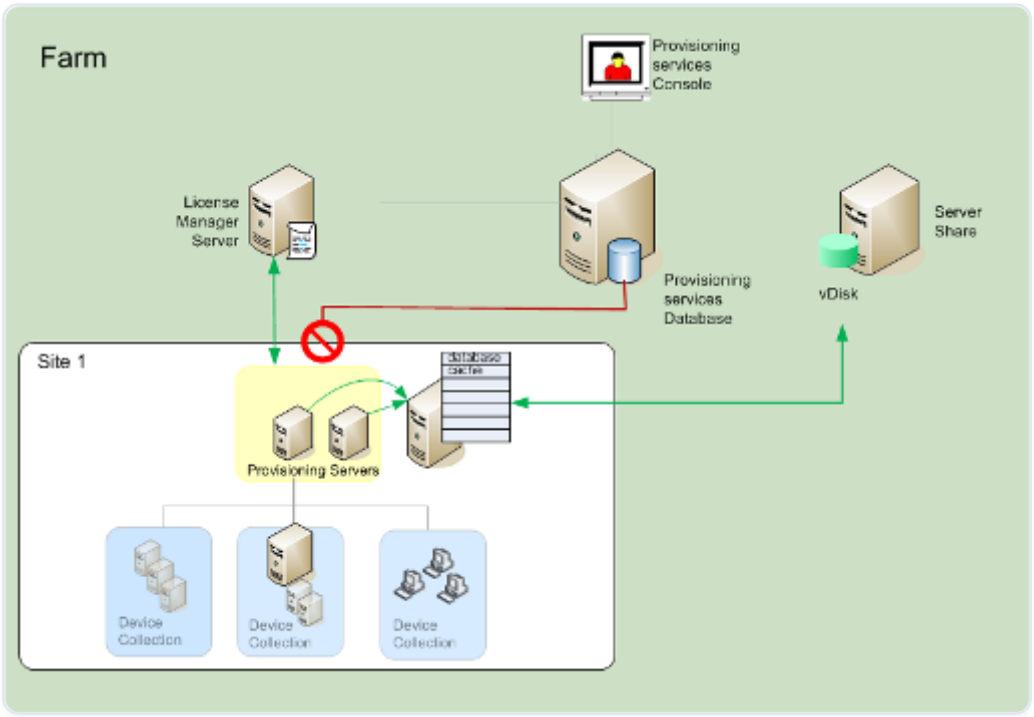
When offline database support is enabled on the farm, a snapshot of the database is created and initialized at server startup. The Stream Process continually updates the snapshot.

When the database becomes unavailable, the Stream Process uses the snapshot to get information about the Citrix Provisioning™ server and the target devices available to the server. This process allows servers and target devices to remain operational. However, when the database is offline, management functions and the console become unavailable.

> **Tip:**

> The snapshot for offline database support is in memory. However, the offline database support option might not work if the database is partially available, or otherwise responds poorly or in an unexpected manner.

> When the database connection becomes available, the Stream Process synchronizes any server or target device status changes made to the snapshot, back to the database.



Considerations

These features, options, and processes remain unavailable when the database connection is lost, even if the **Offline Database Support** option is enabled:

- AutoAdd target devices
- Virtual disk updates
- Virtual disk creation
- Active Directory password changes
- Stream Process startup
- Image Update service
- Management functions: PowerShell, MCLI, SoapServer, and the Console

Enabling offline database Support

1. In the Citrix Provisioning console tree, right-click on the **Farm**, then select **Properties**. The **Farm Properties** dialog appears.
2. On the **Options** tab, select the **Offline Database Support** check box.
3. Restart Stream services.

Database mirroring

If you mirror a Microsoft SQL database and the primary version becomes unavailable, Citrix Provisioning™ supports the mirrored version, resulting in improved overall availability.

Database mirroring can be implemented in a new or existing farm and requires the following high-level tasks:

- Creating the Citrix Provisioning MS SQL primary database (created when running the Installation Wizard on the server)

  > **Note:**
  >
  > For database mirroring to function, the recovery model must be set to **Full**.

- Identifying the primary database server and instance (identified when running the Configuration Wizard)
- Identifying an existing MS SQL failover database server (identified, not created, when running the Configuration Wizard)
- Configuring mirroring between the primary and failover database servers (configured using MS SQL database server tools)

Citrix recommends that you start the failover server before enabling database mirroring in the farm. For information, see Windows Server Failover Clustering with SQL Server.

> **Tip:**
>
> Use the information in this article configure database mirroring using the configuration wizard.

> Run the Configuration Wizard to specify the new failover server so that the status of the Citrix Provisioning farm correctly reports the new settings. After rerunning the wizard, some services, including the stream service, restart so that the farm has the new failover server settings.

Enabling mirroring when configuring a New Farm

1. Start the Configuration Wizard on a server that resides in the new farm.

2. While running the wizard, when the **Farm Configuration** screen displays, select the **Create Farm** radio button to create a farm, then click **Next**.
3. On the **Database Server** screen:
    a. Type or use the **Browse** button to identify the primary database server and instance names.
    b. Select **Active Directory Integrated** authentication if you want to use the services' user account. Enter the database credentials that the Stream and SOAP services will use.
    c. Click **Connections Options...**
4. On the **Database Connection Options** screen:
    a. Select **Specify database mirror failover partner** check box.
    b. Type or use the **Browse** button to identify the failover database server and instance names. Optionally, enter a TCP port number for communication with this server.
5. Click **OK**. If the failover database was previously configured and is running, Citrix Provisioning connects to it. If the failover database server has not been created or is not running, an error message displays, indicating a failure to connect. In this case, when prompted, click **Yes** to continue (the failover database can be created and configured after the new farm is created).
6. On the **Database Server** screen, click **Next**.
7. Enter database administrator credentials in the pop-up dialog. Select **Active Directory Integrated** authentication if you want to use the current login. Click **OK**.
8. On the **New Farm** page, enter a name for the new database on the primary database server, then complete any additional requested information.
9. Click **Next**.
10. Complete the remaining wizard pages.

Enabling mirroring within an existing Farm

To enable mirroring within an existing farm:

1. Confirm that the primary and failover database servers are up and running.
2. Using MS SQL server tools, mirror the Citrix Provisioning database to a database on the failover database server.
3. Run the Configuration Wizard on each server.

4. Identify the farm by choosing either the **Farm is already configured** or the **Join existing farm** option on the **Farm Configuration** page.
5. On the **Database Server** screen:
    a. Type or use the **Browse** button to identify the primary database server and instance names.
    b. Select **Active Directory Integrated** authentication if you want to use the services' user account. Enter the database credentials that the Stream and SOAP services will use.
    c. Click **Connections Options...**
6. On the **Database Connection Options** screen:
    a. Select **Specify database mirror failover partner** check box.
    b. Type or use the **Browse** button to identify the failover database server and instance names. Optionally, enter a TCP port number for communication with this server.
7. On the **Database Server** screen, click **Next**.
8. Enter database administrator credentials in the pop-up dialog. Select **Active Directory Integrated** authentication if you want to use the current login. Click **OK**.
9. Complete the remaining wizard pages.

SQL Always On for SQL Server 2012, 2014, 2016, 2017 and 2019

Citrix Provisioning™ supports the SQL Always On high availability and disaster recovery solution. Consider the following:

- The Microsoft OLE DB Driver for SQL Server is required. It is installed when you install Citrix Provisioning server.
- Citrix Provisioning is only aware of and interacts with Always On through the listener DNS name.
- The database must be part of the pre-made high availability group.
- The listener DNS name and high availability group are part of the procedures to create SQL Always On.
- The soap/stream services user must be manually configured to have full permission to each SQL server part of the Always On configuration.
- Citrix Provisioning is not aware of the individual SQL server/cluster behind SQL Always On.

Note:

See Supported Databases for XenApp and XenDesktop Components in the Knowledge Center for additional information about supported databases and clients.

Provisioning server failover

All Citrix Provisioning™ servers within a site that can access a virtual disk provide the disk to target devices. On shared storage, multiple servers access the same physical files, allowing a target device to establish a connection on an alternate server.

This *failover* permits a connection to the active server if the connection is interrupted for any reason. When failover occurs, a target device does not experience any disruption in service or loss of data.

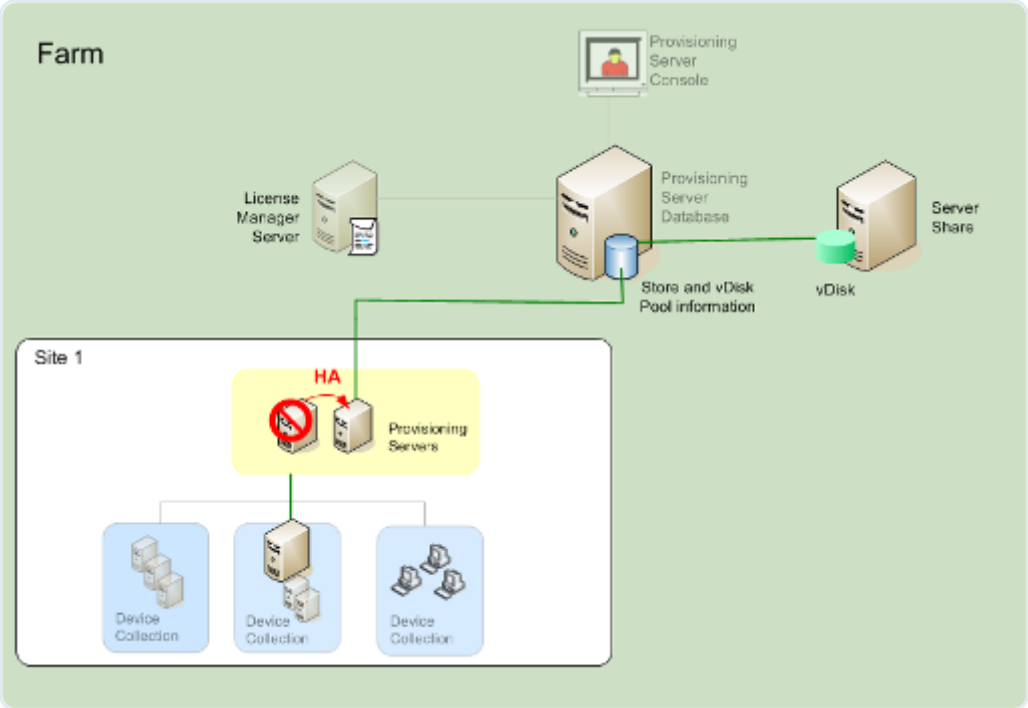
Note:

If a server failover occurs, only those servers with access to an identical replicated virtual disk provide that virtual disk to target devices. For example, if a virtual disk is replicated across three servers and one of the them is updated, that virtual disk is no longer identical. It is not considered if a server failover occurs. Even if the same exact update is made to two of the virtual disks, the timestamps on each differ, resulting in disks that are no longer identical.

Citrix Provisioning does not support virtual disk high availability on local storage in Private Image mode or vDisks that are currently in maintenance mode.

If load balancing is enabled and a server providing that virtual disk fails, the load is automatically balanced between the target device and the remaining servers. When load balancing is not enabled, a single server is assigned, providing the virtual disk to target devices. In such situations failover does not occur.

For information on automatically balancing the target device load between servers, see Managing Servers.



The server accessed by the target device does not necessarily become the one that accesses the virtual disk. Once connected, if one or more servers can access the virtual disk for this target device, the server that is least busy is selected.

To force all target devices to connect to a different server, stop the Stream Service on that server. Upon shutdown, the Stream Service notifies each target device to relogin to another server.

Testing target device failover

To ensure that devices can failover successfully, complete the following:

1. Double-click the **vDisk status icon** on the target device; note the IP address of the connected Citrix Provisioning server.
2. Right-click the connected server in the Citrix Provisioning console. Select **Stream Services**, then click **Stop**.
3. Confirm that the IP address of the connected server changes to that of an alternate server in the virtual disk status dialog.

Configuring for high availability with shared storage

Citrix Provisioning™ servers are configured to access your shared-storage location, and supports various shared-storage configurations. The configuration steps for highly available storage in the network vary depending on shared-storage configurations.

Windows shared-storage configuration

When using a Windows shared storage location, service account credentials (user account name and password) must be a domain account that is configured on each Citrix Provisioning server. This method is used to access the Stream Service and the shared storage system.

Creating stream service account credentials on the domain controller

The stream service runs under the user account. When the stream service accesses a virtual disk stored locally on the server, the local user rights provide full access. However, when the database or virtual disk is on a remote storage device, the streaming server must use a domain account with rights to both the provisioning server and the remote storage location. An administrator must assign full control rights to the stream service account in order for it to read and write to the remote storage location.

An administrator creates service account credentials in Active Directory and assigns the credentials to the stream service on all Citrix Provisioning servers that participate in high availability. Alternatively, an existing domain user account can be given full control rights to the network share and be assigned to the Stream Service.

Consider the following when creating service account credentials:

- You must be logged on as an administrator or a member of the Administrator group to create a domain account.
- Clear the User must change password at next logon check box.

Assigning stream service account credentials manually

When running the Configuration Wizard on a provisioning server, you are prompted to enter an account name and password for the Stream Service to use. This account must have access permissions for any stores it is given access to, in addition to permissions in SQL Server for database access. If necessary, credentials can be assigned manually.

To assign the Service account credentials to the Stream Service:

1. Open the **Windows Control Panel**.
2. Go to Administrative **Tools > Services**.
3. Double-click on the first Citrix Provisioning Stream Service name in the Services list.
4. On the **Log On** tab, select **This Account**, then click **Browse**.
5. Click **Locations**, select the **domain node**, then click **OK**.
6. Type the name of the Stream Service user account, then click **Check Names**.

7. Click **OK** to close the **Select User dialog**.
8. On the **Log On** tab, enter and confirm the Stream Service account password, then click **OK**.
9. After assigning the Service account credentials to the Stream Service, restart the Stream Service.

Configuring storage access

The stores that contain the vDisks must be shared, and the Service account credentials need to have access to remote storage for vDisks, with the appropriate permissions.

To share your virtual disk's stores folders, and grant access permissions to your Service account credentials:

1. In Windows Explorer, right-click on the folder that contains the database and virtual disk folders. For example, if the database and virtual disk files are stored in the default C:\Program Files\Citrix\Provisioning Services folder, right-click on that folder.
2. Select **Sharing and Security** from the shortcut menu.
3. Enable the **Share this folder** radio button, then optionally enter a share name, and comment.
4. Click **Permissions**.
5. If the Service account credentials user name does not appear in the Group or user names list, click **Add**. Enter the user name of the Service account credentials, and click **Check Names** to verify.
6. Click **OK**.
7. Select the service account credentials user name.
8. Enable the **Full Control** check box (the **Full Control** check box and all additional check boxes are selected).
9. Click **Apply**.
10. Select the **Security** tab.
11. If the Service account credentials user name does not appear in the Group or user names list, click **Add**. Enter the user name of the Service account credentials, then click **Check Names** to verify.
12. Click **OK**.
13. Select the **Service account credentials** as the user name.
14. Enable the **Full Control** check box, then click **Apply**.
15. Click **OK**.

SAN configuration

If you are storing the database and vDisks on a SAN, use local system accounts for the Stream Service. Unlike a Windows network share, creating special Service Account Credentials to guarantee access to your data is not necessary to guarantee access to your data.

Usually, a SAN configuration allows setting up as if the database and vDisks were stored locally on the Citrix Provisioning server.

Configuring the boot file for high availability

A Citrix Provisioning™ server can be selected as one of the servers used to connect target devices during the boot process. For a configuration to be highly available, at least two login servers must be listed in the boot file (maximum of four servers).

The target device boot file contains the IP addresses of up to four login servers, in addition to other configuration information. The boot file lists the servers that a target device can contact to gain access to the Citrix Provisioning farm. The contacted server delivers the target device to a different server, which can provide the target device with its virtual disk.

> **Note:**
>
> A shared storage system ensures the availability of the Citrix Provisioning server vDisks. Depending on the type of shared storage, the vDisks use either the Universal Naming Convention (UNC) or the usual DOS naming convention.

Adding Citrix Provisioning servers to the boot file

Add servers to the boot file to provide a target device with the information necessary to contact the Stream Service.

When configuring a server, the wizard allows you to select the server for TFTP services. There is one TFTP server per farm. If target devices are on multiple network segments, and each segment is configured as an independent site, then one TFTP server per site (network segment) is used.

Troubleshooting

Use the information in this section to troubleshoot Citrix Provisioning™ components:

- Logging
- Auditing
- APIs
- CIS Problem Reporting

Logging

Citrix Provisioning™ uses diagnostic tools for troubleshooting and managing a provisioning farm. These tools allow you to report a problem or use SQL Server Always On Tracing (AOT).

Report a problem

Use Citrix Insight Services (CIS) problem reporting to directly report problems you encounter to Citrix Support. CIS is a platform for instrumentation, telemetry, and business insight generation. For more information, see CIS Problem Reporting.

> **Tip:**
>
> For details and the latest information about CIS and how it works, see the CIS website. Citrix account credentials are required to log in.

Always on Tracing

Citrix Provisioning Always on Tracing (AOT) functionality allows you to store AOT logs directly to the disk. You do not need to enable the feature because this feature is enabled by Citrix Provisioning and is continuously running. If there is an issue, collect the problem report that has the logs from the time when the problem occurred.

Auditing

Citrix Provisioning™ provides an auditing tool that records configuration actions on components within the provisioning farm. The auditing tool saves this information to the provisioning database. It provides administrators with a way to troubleshoot and monitor recent changes impacting system performance and behavior.

Administrator privileges determine viewable audit information and visible menu options. For example, a *farm administrator* views audit information within the farm. This functionality is unlike a *device administrator* who only views audit information for those device collections for which they have privileges.

> **Note:**
>
> Auditing is off by default. If the Citrix Provisioning database is unavailable, no actions are recorded.

To enable auditing

1. In the **Citrix Provisioning console** tree, right-click on the farm, then select the **Farm Properties** menu option.
2. On the **Options** tab, under **Auditing**, check the **Enable auditing** check box.

The following managed objects within a Citrix Provisioning implementation are audited:

- Farm
- Site
- Provisioning servers
- Collection
- Device
- Store
- vDisks

Recorded tasks include:

- Citrix Provisioning console
- MCLI

- SOAP Server
- PowerShell

Accessing auditing information

Auditing information is accessed using the provisioning console. You can also access auditing information using programmer utilities included with the product installation software:

- MCLI programmer utility
- PowerShell programmer utility
- SOAP Server programmer utility

In the console, a farm administrator can right-click on a parent or child node in the console tree to access the audit information. The audit information that other administrators can access depends on the role they were assigned.

To access auditing information from the Citrix Provisioning console

1. In the Citrix Provisioning console, right-click on a managed object, then select the **Audit Trail** menu option. The **Audit Trail** dialog displays or a message appears indicating that no audit information is available for the selected object.
2. Under **Filter Results**, select from the filter options, which enable you to filter the audit information based on, for example, **user**.
3. Click **Search**. The resulting audit information displays in the audit table. Columns can be sorted in ascending and descending order by clicking the **Column** heading:
    - **Action list number:** Based on the filter criteria selected, the order the actions took place.
    - **Date/Time:** Lists all audit actions that occurred within the **Start date** and **End date** filter criteria.
    - **Action:** Identifies the name of the Citrix Provisioning action taken.
    - **Type:** Identifies the type of action taken. This action is based on the type of managed object for which the action was taken.
    - **Name:** Identifies the name of the object within that object's type, for which the action was taken.
    - **User:** Identifies the user's name that performed the action.
    - **Domain:** Identifies the domain in which this user is a member.

- **Path:** Identifies the parent of the managed object. For example, a device has a site and collection as parents.

4. To view more details for a particular action, highlight that action's row within the results table, then click one of the option buttons that follow:

   - **Secondary:** Any secondary objects that this action affected. This option opens the **Secondary** dialog, which includes the type, name, and path information. This dialog allows you to view secondary object actions such as parameters, sub actions, and changes.
   - **Parameters:** Any other information used to process the action. This option opens the **Parameters** dialog. It includes the parameter name, representing the object, and the value.
   - **Sub Actions:** Extra actions that were performed to complete this action. This option opens the **Sub Actions** dialog, which includes action, type, name, and path information.
   - **Changes:** Any new or changed values (such as ‘Description’) associated with the object (such as a target device). This option opens the **Changes** dialog, which includes the name and new information.

Archiving the audit trail information

The farm administrator determines how long to make the audit trail information accessible before it is archived.

To configure the audit trail archiving

1. In the console, right-click on the farm, then select **Archive Audit Trail**. The **Archive Audit Trail** dialog appears.
2. Browse to the saved location where audit trail information resides (XML file). The **Select File to Archive Audit Trail To** dialog opens.
3. Select the location, then type the name of the new file in the **File name** text box.
4. Open the calendar from the **End date** menu, then select the date on which the audit trail information is archived. The default is the current date.
5. To remove all audit information, select the **Remove information archived from the Audit Trail** check box. Once the information is removed, it can no longer be accessed directly from Citrix Provisioning. It exists in the XML file.
6. Click **OK**.

APIs

Citrix Provisioning APIs are available on the Citrix Developer Documentation site:

- SOAP Server Programmer's Guide
- PowerShell with Object Programmer's Guide

PowerShell SDK files after upgrading

Files located in `C:\Program Files\Citrix\PowerShell SDK` are missing after upgrading. This issue occurs because the CDF version used by Citrix Provisioning does not match the version used by other components associated with Citrix Virtual Apps and Desktops. As a result, newer CDF files have a lower version number than previous ones. This issue does not affect the functionality of importing CPV device collections into CVAD machine catalogs. To resolve this issue:

1. Close Citrix Studio.
2. Mount the new Citrix Virtual Apps and Desktops™ ISO.
3. In the mounted ISO, navigate to \x64\DesktopStudio.
4. Right-click **PVS PowerShell SDK x64** to expose a contextual menu.
5. Select **Repair**.
6. Run the Repair option. The installation adds the two CDF files as needed.

Active Directory group enumeration method

The Citrix Provisioning™ console contains the Citrix Virtual Apps and Desktops Setup Wizard, providing integration tasks between Citrix Provisioning, Citrix Virtual Apps and Desktops, and Windows Active Directory. The Wizard creates the VMs and any necessary objects in Citrix Provisioning, Citrix Virtual Apps and Desktops and Windows Active Directory.

> **Note:**
>
> This implementation was limited in earlier releases due to the absence of an exposed API. Without it, Citrix Provisioning users cannot run various automated testing paradigms in their environments.

> Citrix Virtual Apps™ and Desktops and Streamed VM Wizard functionality are exposed by a service on the Provisioning Server through a PowerShell API. This API provides a PowerShell front end. It can be used to automate the functionality provided by the Streamed VM Setup Wizard and the Citrix Virtual Apps and Desktops Setup Wizard.

> **Tip:**
>
> The Citrix Provisioning API service uses an SSL connection which requires you to configure an X.509 certificate on the Provisioning Server.

Configure the X.509 certificate

The Citrix Provisioning API service uses an SSL connection requiring an X.509 certificate on the provisioning server. The certificate's CA certificate must also be present on the server and console machine.

To create a self-signed certificate for Citrix Provisioning API:

1. Download and install the Windows SDK for your provisioning server operating system.
2. Open a command prompt and navigate to the bin folder of the SDK. By default: `C:\Program Files (x86)\Windows Kits\SDK_Version\bin\x64>` and run the following commands.
3. Create a certificate to act as your root certificate authority: `makecert -n "CN= PVSRoot CA" -r -sv PVSRoot CA.pvk PVSRoot CA.cer`.
4. Create and install the service certificate: `makecert -sk PVSAP I -iv PVSRoot CA.pvk -n "CN= FQDN of the PVS Server" -ic PVSRoot CA.cer -sr localmachine -ss my -sky exchange -pe`.
5. Install the root CA certificate in the `Trusted Root Certification Authorities` location on the server and console Machines: `cert mgr -add "PVSRoot CA.cer" -s -r localMachine Root`.
6. Run the Configuration Wizard. On the **Soap SSL Configuration page**, select the created certificate.

> **Note:**

> When you run PowerShell commands, use the *FQDN of the PVS Server* for `PvsServerAddress` and 54324 (default) for `PvsServerPort`.

Citrix Provisioning API

To use the Provisioning API with Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), you must provide credentials to authenticate to Citrix Cloud.

Use the Provisioning API with Citrix DaaS™

When using Citrix DaaS, the Provisioning API service running on each provisioning server requires credentials to authenticate to Citrix Cloud. After you provide these credentials, any process running with the specified user name uses the secure client credentials to authenticate to Citrix Cloud.

To provide these credentials:

1. Log in to the Citrix Cloud portal IAM page as an admin user.
2. Create a secure client from the Citrix Cloud IAM page. From this page, also record your customer ID.
3. Download the secure client to a CSV file on the PVS server.

> **Important:** The CSV file contains a secret that can be used to authenticate to Citrix Cloud as the user who created the secure client. Save and protect this file.

4. On each server that runs Provisioning API calls:
    a. Run a PowerShell window using the Provisioning Services user name.
    b. Download the CSV file.
    c. Run this command:

```
Set-XDCredentials -CustomerId "<customerIDFromPortal>"
-SecureClientFile "<CSVPath>" -ProfileType CloudAPI –StoreAs
"default"
```

    d. Delete the downloaded copy of the CSV file.

Use the Citrix Provisioning API

After installing the latest Citrix Provisioning server:

1. Run the configuration wizard.
2. Open the **Services** window on the provisioning server and verify that the Citrix Provisioning API is installed and configured to run as an administrator.

> **Tip:**
>
> The Citrix Provisioning API service uses an SSL connection which requires you to configure an X.509 certificate on the provisioning server.

Open a **PowerShell** window on your provisioning server and import the command module:

1. `Import-Module "C:\Program Files\Citrix\Provisioning Services\Citrix.ProvisioningServices.dll"`.
2. `Get-Command-Module Citrix.ProvisioningServices`.
3. Ping the Citrix Provisioning API service: **Get-PvsApiServiceStatus -PvsServerAddress *FQDN of PVS Server* -PvsServerPort** *Port PVS API is configured to listen on*

> **Tip:**
>
> The provisioning server port number is the one used for SOAP server communication.

Log in to the Citrix Provisioning API (use either of the following commands):

Use Domain/Username/Password parameters:

`Get-PvsConnection -PvsServerAddress` *FQDN of PVS Server* `-PvsServerPort` *SOAP Port +1 PVS API is configured to listen on* `-Domain` *PVS Admin Domain* `-Username` *PVS Admin user name* `-Password` *PVS Admin password*

Use Pass-in PSCredential object:

`Get-PvsConnection -PvsServerAddress` *Address of PVS Server* `PvsServerPort-Credentials` *PSCredential Object returned by Get-Credential*

The following cmdlets are included with the Citrix Provisioning API implementation:

- **Get-PvsApiServiceStatus.** Pings the service to determine whether the service is up and running at a particular address/port.
- **Get-PvsConnection.** Log into the Citrix Provisioning API.
- **Clear-PvsConnection.** Logout of Citrix Provisioning API. This cmdlet adds the **Auth Token** to the block list.
- **Start-PvsProvisionXdMachines.** Used for Citrix Virtual Apps and Desktops Setup Wizard automation.
- **Start-PvsProvisionMachines.** Used for Streaming VM Setup Wizard automation.
- **Get-PvsProvisioningStatus.** Uses the ID returned from either of the previous two commands to get the status of the current provisioning session.
- **Stop-PvsProvisionMachines.** Uses the ID returned from either of the previous two commands to cancel the current provisioning session.

You can access examples for these PowerShell cmdlets using `Get-Help CommandName –Examples`:

> **Tip:**
>
> Do not use the other PowerShell commands because they are all part of the Database Access layer.

When connecting to the API using the `Set -PvsConnection` PowerShell command, a connection object is returned, resembling:

Within Citrix Provisioning, the user access control method is based on the user's Active Directory login credentials and the administrative group configuration. As a result of this method, AD group enumeration repeatedly triggers events associated with Configuration Wizard and Console operations. In complex AD environments where spurious logins can occur, the system can become sluggish, with slow responses resulting in connection timeouts to the Citrix Provisioning console.

This functionality resolves such issues by improving the method responsible for AD group enumeration.

Before this functionality, AD group enumeration occurred by scanning memberships associated with the user's login in its domain and the entirety of the trusted domains. This process continues until all the user's group memberships are determined, or if there are no additional domains to search. The identified groups are compared to the administrative groups defined in the database to determine the user's access rights.

With this functionality, AD group enumeration is enhanced to intelligently search preferred domains for a user's login memberships. This approach is different than searching the entirety of groups over all domains. The administrative group name associated with the user's login credential is used to provide the preferred domain list. The user's domain list is searched first, followed by the preferred list. During this search, if a farm's administrative group is discovered, the search halts because the user already has full access rights to the Citrix Provisioning farm. This search paradigm also includes a mechanism that uses the domain security ID to verify if the domain contains the intended groups. This modified searching approach of domains for a user's login membership addresses the needs of most AD environments, resulting in faster Configuration Wizard and provisioning console operations.

Use BDM PowerShell

1. Open a PowerShell window on your provisioning server and run `installutil.exe` to make the BDM PowerShell commands available.

```
PS C:\Users\Administrator.MCU> c:
\Windows\Microsoft.NET\Framework64\v4.0.30319\installutil.exe 'C:
\Program Files\Citrix\Provisioning Services\BdmPowerShellSdk.dll'
```

2. Run the following to get help on running the commands to create a boot device manager.

```
PS C:\Users\Administrator.MCU> get-help -examples New-BootDeviceManager
```

CIS Problem Reporting

Citrix Provisioning™ allows you to report problems you encounter with servers and sites. The support team uses the information to troubleshoot and diagnose the problem to improve Citrix Provisioning.

How problem reporting works

Problem reporting works by sharing diagnostic information resulting from an event within Citrix Provisioning. It can be performed for a specific Citrix Provisioning server, or for a site:

- If you have an environment with multiple provisioning servers, each has a different SOAP Service user. In such environments, the SOAP Service user must have read\write permissions to the network share when generating the diagnostic bundle.
- If you are reporting a problem for a specific provisioning server, only that server generates a diagnostic bundle that captures the event.
- If you are reporting a problem for a site, each provisioning server in the site generates a diagnostic bundle.
- Save the diagnostic bundle to a shared network drive.

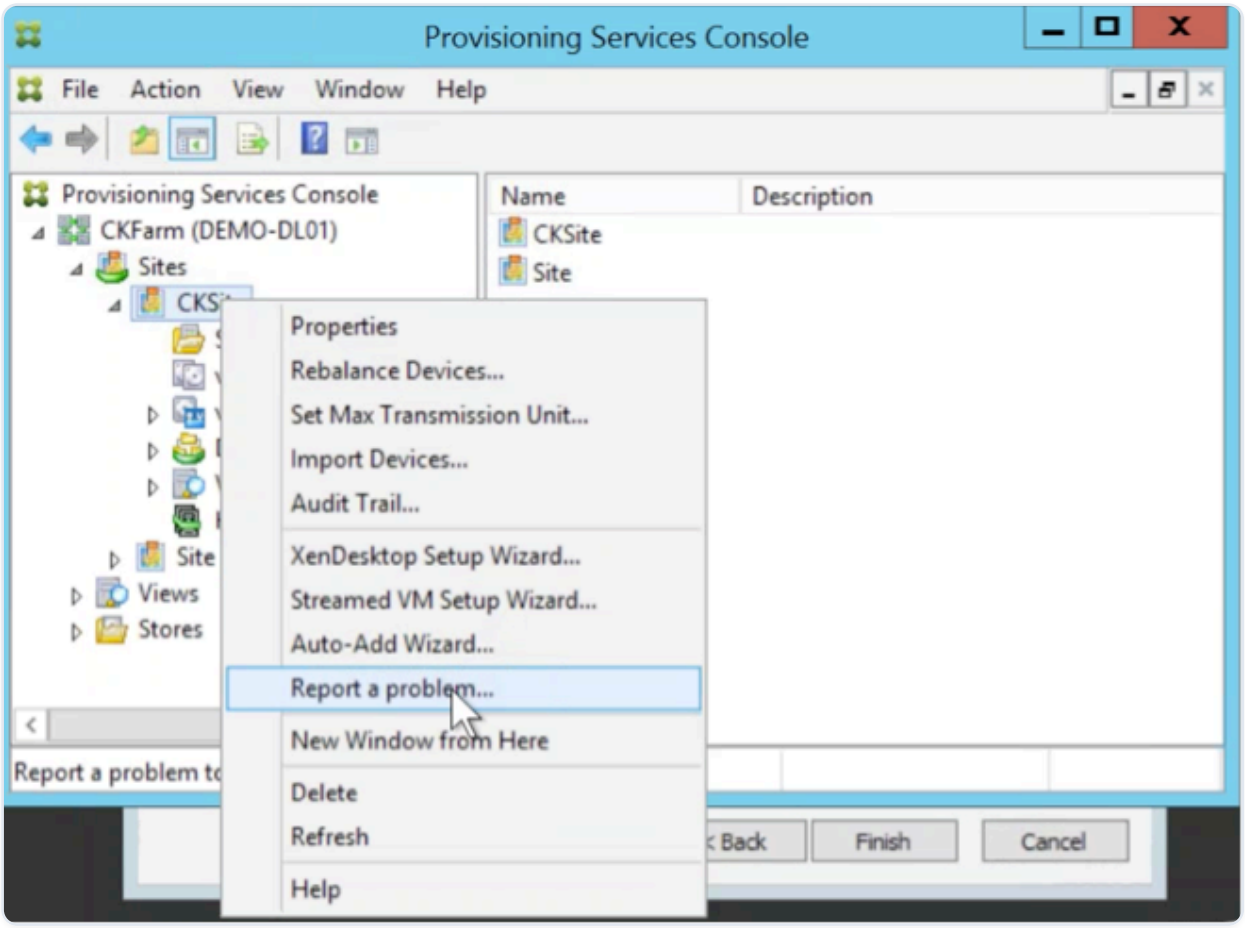
> **Note:**
>
> Citrix® customer support provides instructions on making the diagnostic bundle available to them.

Report a problem

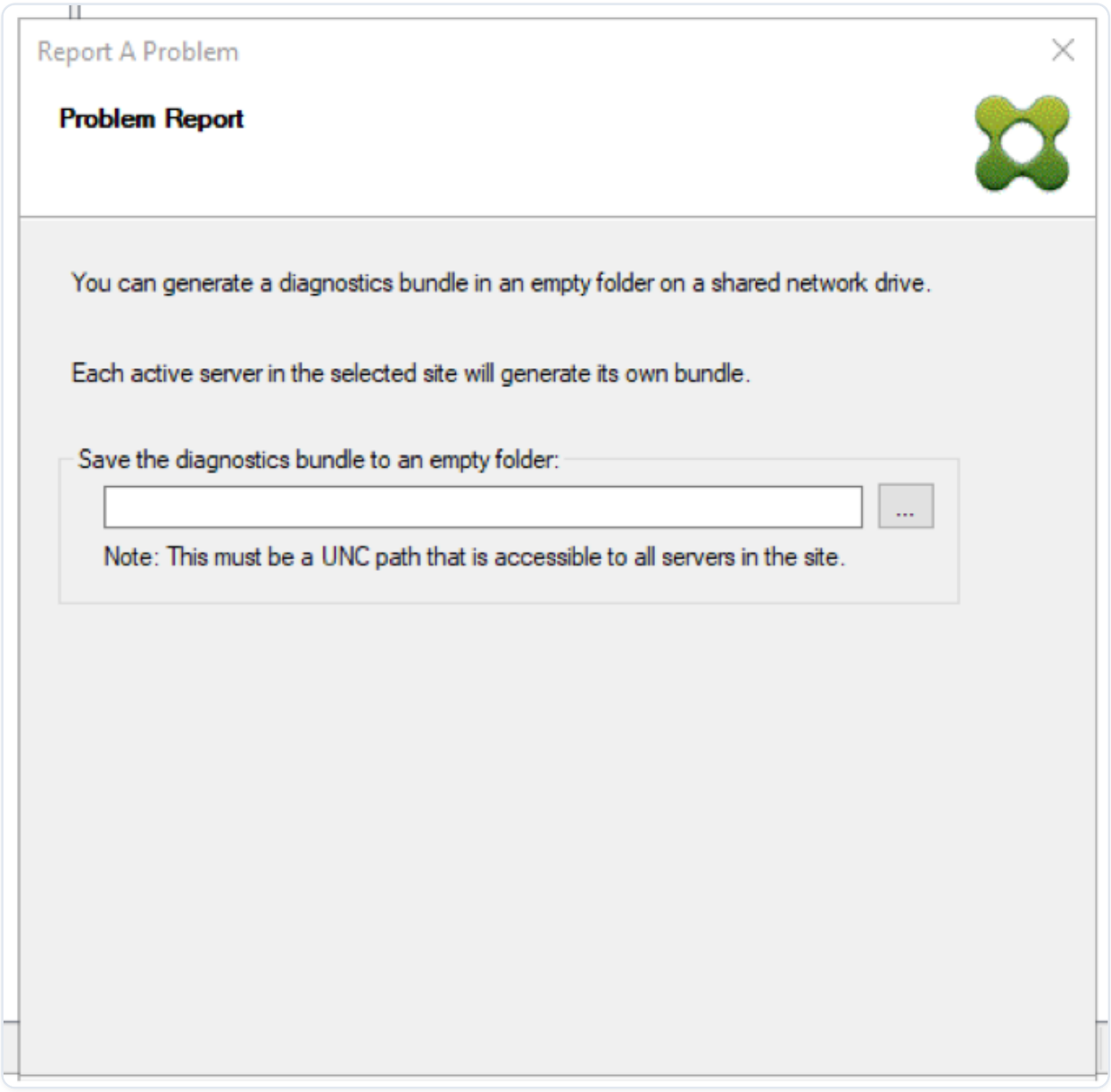
You can generate diagnostic information locally to a ZIP file. Select an empty folder on a shared network drive accessible to all servers included in the problem report.

To report a problem

1. In the **Citrix Provisioning Console**, expand the **Sites** node to display the server on which you want to report a problem.
2. Right-click a server to display a contextual menu.
3. Click **Report a problem**.



4. In the **Problem Report** screen, save the diagnostic bundle to an empty folder. This must be a Universal Naming Convention (UNC) path that is accessible to all servers in the site.



5. Click **Next**.

> **Note:**
>
> Each server in the selected site generates its own diagnostic bundle.

6. Specify information to help describe the issue. In the **Specify Problem Details** screen:

   a. Enter a brief description that summarizes the problem. Once you enter the information for this mandatory field the remaining fields become editable.

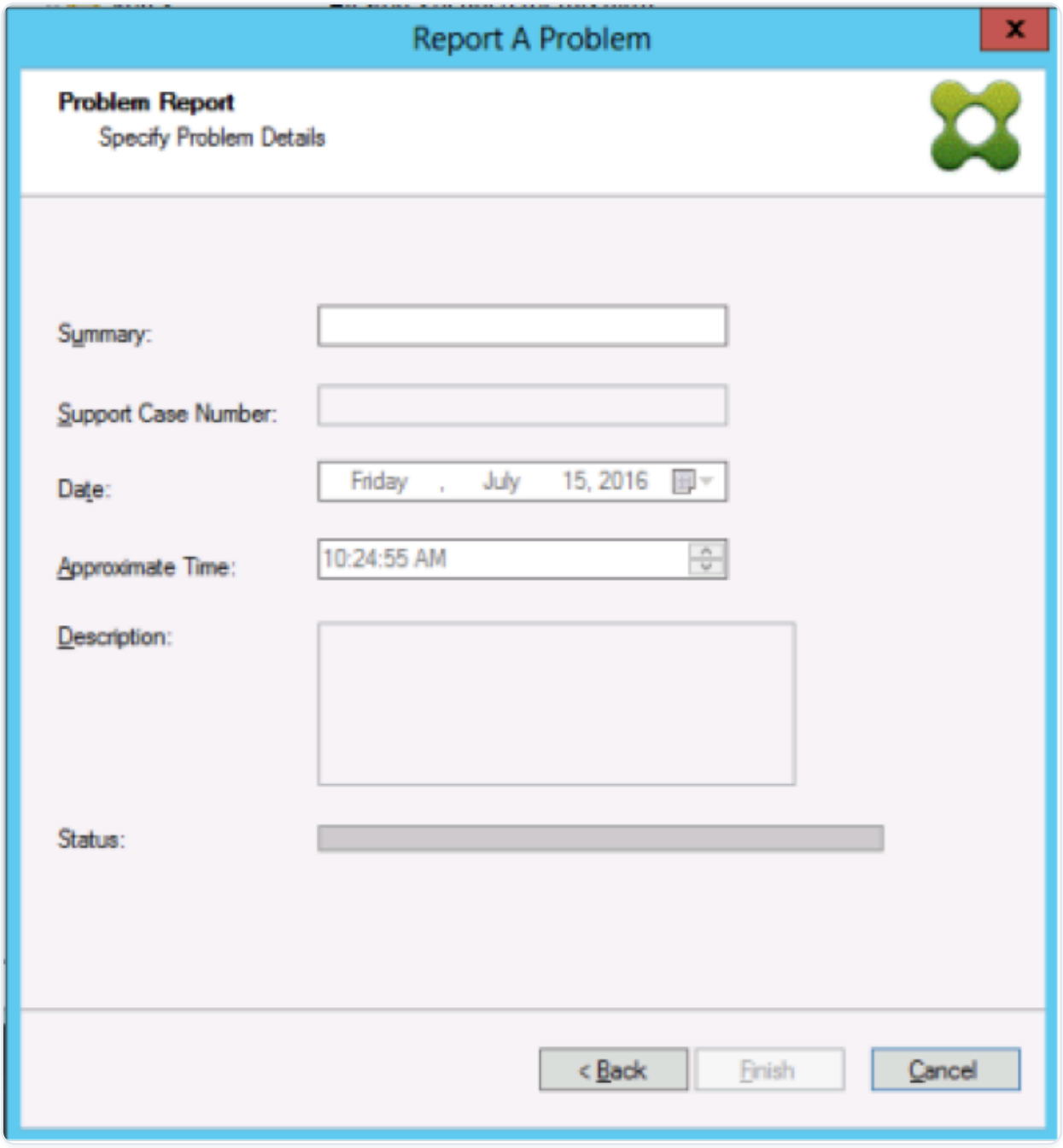
   b. Enter a support case number (optional).

   c. Select the date when the problem occurred.

d. Enter an approximate time when the problem occurred.

e. Enter a description that characterizes the problem.

7. Click **Finish**.

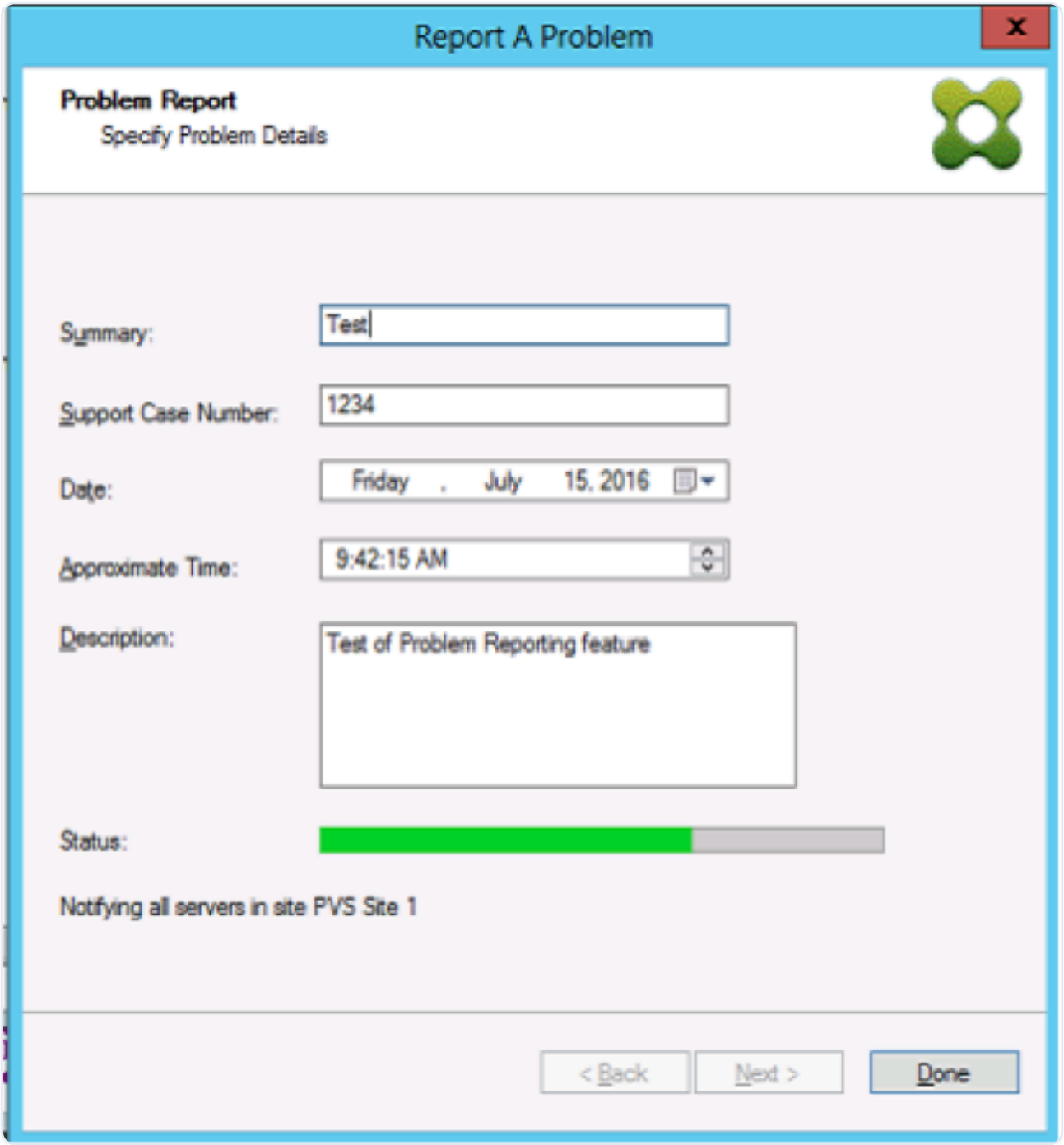


Tip:

After finishing the diagnostic report, the bundle is created on the server. You can view the status of the most recent problem report from **Server>Property>Problem Report**.

After clicking **Finish**, the problem reporting function reports the issue for either a single server, or for each server in a site. Each server generates the problem report as a background task and saves the file to a shared network drive.

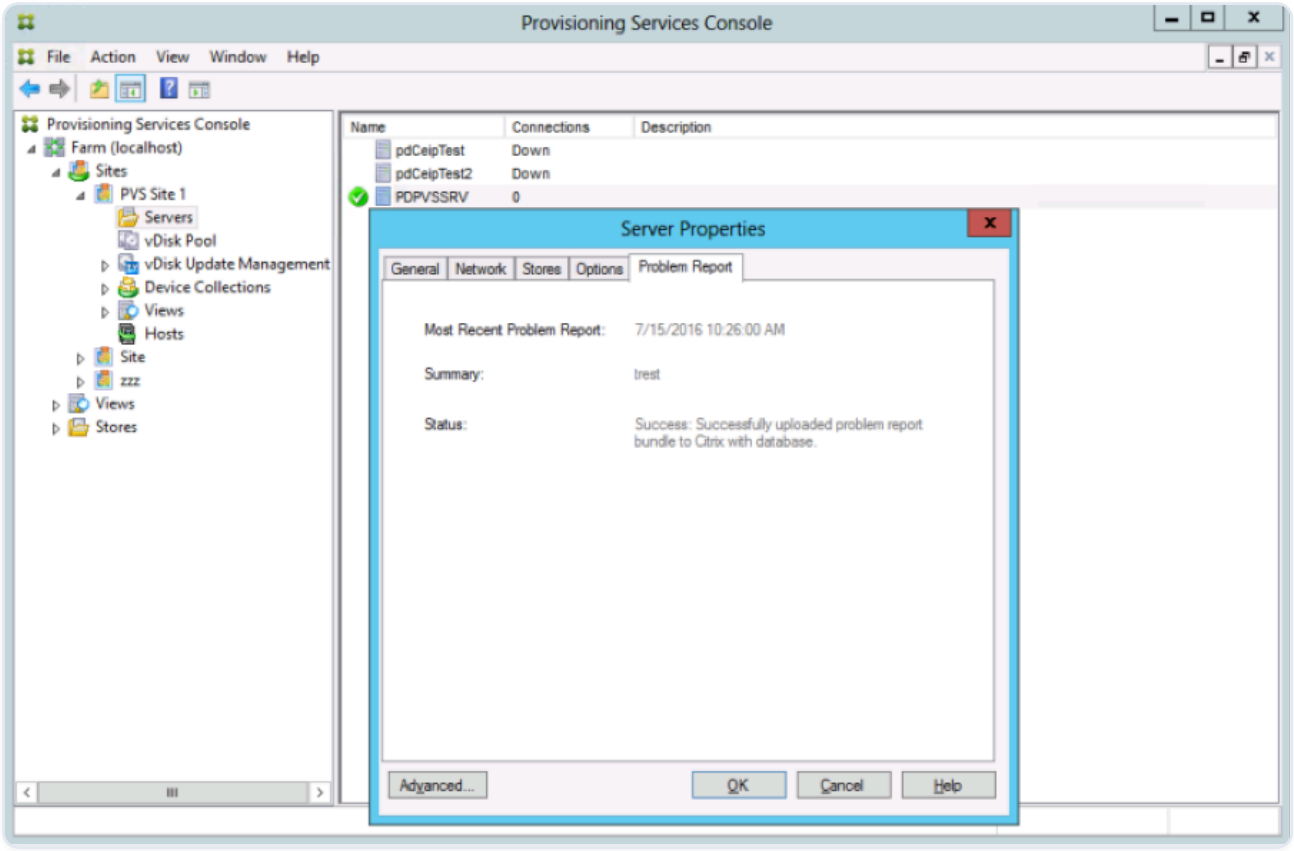
The **Status** field displays information about the state of the reporting progress. After the process starts, click **Done** to dismiss the dialog, and allow the process to continue in the background:



If you choose not to dismiss the dialog, the process continues in the foreground. After the report completes, the **Problem Report** screen provides additional information *Check each Server's Properties for results.* This message indicates that each server has completed its problem report and saves the results.

.png)

After the problem report is generated, you can view the results on the **Properties** screen. To view the report, select **Server>Properties**.



The **Problem Report** tab displays:

- **Most recent problem report**. This field displays the date and time of the most recent problem reporting attempt.
- **Summary**. This field describes the problem. The information is generated from the mandatory summary field specified when the administrator first created the report.
- **Status**. Describes the status of the most recent report. It indicates:
  - Success or failure
  - Whether the report was saved to a shared network drive. If so, the full path to the file is displayed.

Migrate VM to a new hosting resource

You can migrate VMs provisioned with Citrix Provisioning and without changing the Citrix Virtual Apps and Desktops™ and provisioning power functions. You might migrate the VM when you are

retiring a hosting resource and want to migrate the provisioned VMs to a new hosting resource instead of provisioning new VMs.

> **Important:** After you migrate the VM, the provisioned MCS catalog in the old host no longer works.

> Shut down the VM. Then, do these processes in any order:

- Edit the hosting unit.
- Change the host resource to point to your new hosting resource.
- Migrate the provisioned VM from your old hosting resource to the new one.

When you have finished performing these processes, test your VM.

Edit the hosting unit

1. In the Provisioning console, edit the host unit.
2. Change the host address to your new host resource main IP address.
3. On the Credentials tab, change the user name and password to the ones you want to use for the new hosting resource.
4. Click **OK**.

Change the hosting resource

For the provisioning VM to migrate successfully:

- Change the hosting resource to point to your new hosting resource.
- Change the storage to the storage server.
- Specify the new network.

1. Open Citrix Studio.
2. Edit the connection:
    a. On the Hosting tab, select the hosting resource hosting connection and select **Action > Edit Connection**.
    b. In the Connection Properties tab, select **Edit settings**.
    c. In the Edit settings screen, change the address to the new hosting resource pool main IP.

   d. On the Credentials tab, change the user name and password to be used for the new hosting resource pool.
   e. Select **OK**.

3. Change the previously defined storage to the new storage for the hosting resource on your new hosting resource.

   a. Select the hosting resource and select **Action > Edit Storage**.
   b. In the OS Storage tab, clear the local storage location to remove it from use.
   c. Select the new storage server to put it in use.
   d. On the Temporary Storage tab, clear the local storage location and select the new storage location.
   e. Select **OK**.

4. Change the network interface in an existing hosting connection. Still in the Citrix Cloud Connector™, open a PowerShell session with administrator privileges. Run these commands.

   a. Import PowerShell modules: `Add-PSSnapinCitrix*`
   b. Get the host connection details. Note the values for PSChildName and the network path (NewNetworkPath) that are returned: `dir XDHyp:\HostingUnits`
   c. Set the PSChildName to the new hosting resource: `PSChildName = <NewHostingResource>`
   d. Set the network path to the new network: `Set-Item -Path XDHyp:\HostingUnits\<PSChildName> -NetworkPath <NewNetworkPath>`
   e. Run the command that changes the network interface: `Set-Item -Path "XDHyp:\HostingUnits\<NewHostingResource\" -NetworkPath "XDHyp:\Connections\XS2\<New Network Path>`

Migrate the provisioned VM from the old hosting resource to the new one

1. In Citrix Studio, select the provisioned VM.
2. From the context menu, select **Move VM**.
3. Using the wizard, enter values for the following:

   - **Destination:** `<NewHostingResource>`
   - **Target Server:** Not needed
   - **Place all virtual disks on the same:** New storage location

- **Target Network**: `<NewNetworkPath>`
- **Storage Network**: Storage network on new hosting resource

4. Select **Finish**.

Test the migration

To test that the migration was successful:

- Start the VM from the Provisioning console.
- Start the VM from Studio.
- Verify the BDM update. To do so:

  a. Record the IPs in the bootstrap. Configure the bootstrap of the provisioning server that you are currently logged into using invalid IPs.

  b. Enable the bootstrap option **Verbose mode**.

  c. Right-click the HDD BDM-booting provisioned VM and select **Target > Update BDM Partitions**.

  d. Boot the provisioned VM from the Provisioning console.

  e. Verify that the VM is trying to boot from the invalid IP. Shut down the VM.

  f. Configure the bootstrap and fix the IPs in the bootstrap to valid ones. Or, click **Read Servers from database**. Disable verbose mode if necessary. Do the BDM update on the previous client again.

  g. Verify that the VM can boot.

How-to

Create and configure ESD update VMs

VMs that are used to update a Managed vDisk are first created on the hypervisor before configuring for vDisk Update Management in Citrix Provisioning. Supported hypervisors include:

- XenServer®
- Microsoft SCVMM/Hyper-V
- VMware vSphere/ESX

The type of ESD determines the specific steps involved in creating and configuring the VM on the hypervisor.

The following ESD systems are supported:

- WSUS
- SCCM

Following are the general prerequisites to update VMs regardless of the ESD system selected:

1. Download, install, and configure the appropriate ESD Server software on the server.
2. Provide a unique to the VM on the hypervisor and follow naming conventions equivalent to a Citrix Provisioning target device name. The name can be up to 15 bytes in length.
3. Make sure that only one VM exists for a Managed vDisk because only one update task can occur on that vDisk at any given time.
4. Allocate at least 4GBs of memory for each VM.
5. Make sure that appropriate ESD licenses are available and the ESD client software is properly installed and enabled on the vDisk.

> **Note:**
>
> Using Microsoft HyperV Server without SCVMM is not supported.

6. Configure the update VM that is used to build the Update vdisk with a single NIC when streaming to SCVMM.

   Citrix® recommends only applying updates that can be downloaded and installed in 30 minutes or less.

Configure managed vDisks for automated updates

vDisk Update Management uses virtual machines to process updates to managed vDisk(s). vDisks are first created in the Console, then added to vDisk Update Manager as managed vDisks by running the Managed vDisk Setup Wizard.

> **Note:**
>
> If using ESD Servers to deliver updates, the ESD client software must be installed and enabled on the vDisk, and appropriate ESD licensing must also be available.

1. Under the **vDisk Update Management** node in the console tree, right-click vDisks, then select the **Add vDisks…** option. The **Managed vDisk Setup Wizard Welcome** page appears.
2. Click **Next** to begin. The **vDisk** page appears.
3. Select the default search options (All stores, All servers). Or, use the filtering options to select specific stores and/or servers to display the vDisk(s) to select to be managed. vDisks that are not already managed, appear in the vDisk selection box.
4. Select one or more vDisks to be managed, then click **Next**. The **Host/VM** page appears.
5. Select the type of connection to use when hosting the VM, from the appropriate drop-down list.
6. Enter the name of the Update VM used to process the vDisk update. The **VM name** field is case sensitive and must match exactly to the existing VM name on the desired hypervisor.
7. Click **Next**. The Active Directory page appears.
8. If you are using Active Directory, enter a Domain and Organizational Unit to create an Active Directory machine account. This account is used by the Update Device that is created exclusively for updating this vDisk, then click **Next**. The **Confirmation** page appears.

   > **Note:**

> The Update VM should not already pre-exist in the Provisioning Services database or Active Directory. If it does exist, the wizard fails to run.

9. Review all setting, then click **Finish**.

The Managed vDisk Setup Wizard can also be run from the **Managed vDisk** dialog, which displays all Managed vDisks currently in the store. You can run the Managed vDisk Setup Wizard from the **Managed vDisk** dialog by clicking**Add Managed vDisks**.

Create and manage tasks

> **Note:**
>
> The user that configures vDisk Update Management tasks must have permissions to create, modify, and delete Active Directory accounts.

> Use the **Update Task Wizard** to schedule vDisk updates to run automatically:

1. Under the **vDisk Update Management** node in the console tree, right-click **Task**, then select the **Add task…** menu option. The **Update Task Wizard welcome** page appears.
2. Click **Next** to begin configuring a task. The **Name/Description** page appears.
3. Enter a name (required) to identify this task, and a description (optional) in the appropriate text boxes, then click **Next**. The **Schedule** page appears.
4. Select one of the radio buttons to determine how often this task runs: **None**, **Daily**, **Weekly**, or **Monthly**. Depending on which recurrence option was selected, the page displays options specific to that selection:
    - **None**: no additional options appear.
    - **Daily**
        - **Run the update at**: select the time of day to run the daily update from the drop-down menu or enter a specific time.
        - **Everyday**: select to run this daily update everyday of the week: Monday through Sunday.
        - **Weekdays only**: select to run this daily update on weekdays only: Monday through Friday.

- **Weekly**
  - **Run the update at**: select the time of day to run the daily update from the drop-down menu or enter a specific time.
  - Select specific days of the week to run the update.

    > **Note:**
    >
    > Select at least one day to proceed.

- **Monthly**
  - **Run the update at**: select the time of day to run the daily update from the drop-down menu or enter a specific time.
  - Select to run the update task on specific days of the month.

    > **Note:**
    >
    > Only numbers and commas are accepted in this text box. For example: 1 and 15 runs this update task on the first and fifteenth of every month. If either 29 or 31 are entered, this task does not run every month. Or, select On, to select the week and day of the week from the drop-down menus. For example: Selecting First and Monday would run the task on the first Monday of every month.

5. Click **Next**. The **vDisks** page appears.
6. Highlight existing Managed vDisks that updated using this new task, then click **OK**. Optionally, click **Add Managed vDisks** and run the Managed vDisk Setup Wizard to add new managed vDisks to the list. After the wizard completes, the new managed vDisks display in the list and can be selected.
7. Click **Next**. The ESD Client page appears.
8. Select the type of Electronic Software Delivery (ESD) client that is running on the vDisk, from the drop-down list, then click **Next**.

   > **Note:**

> The ESD client software must be installed in the vDisk image. When the option is set to **None**, client-side scripts can be run if the scripts are stored on the vDisk before the update. These scripts must be stored under the installation directory of the client. `Update.bat` is a mandatory script. Optional scripts include `Preupdate.bat` and `Postupdate.bat`, which depend on the users configuration.

9. Optionally, select from the following scripting options, then click **Next**:

   - **Pre-update script**: runs before the start of any update task process.
   - **Pre-startup script**: runs just before startup of the virtual machine.
   - **Post-shutdown script**: runs just after the virtual machine shuts down.
   - **Post update script**: runs after the update task process completes.

   > **Note:**
   >
   > On the server, a subfolder named `Scripts` must be created under the product installation directory. This folder is used to store server-side scripts.

10. On the **vDisk Access** page, select the post-update access mode to assign to the vDisk version, then click **Next**:

    - Leave the vDisk in Maintenance mode (only available to Maintenance Devices)
    - Place the vDisk in Test mode (only available to Test and Maintenance Devices)
    - Make the vDisk ready for use (Production, available to all target devices)

11. Confirm that all vDisk Update Task settings are correct, then click **Finish** to create the task. vDisk Update Tasks can be viewed and modified on the **Update Task Properties** dialog.

Citrix Provisioning™ Document History

The following table lists important changes to this release of Citrix Provisioning. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
08 May 2026	Release of Citrix Provisioning 2402 LTSR CU4	See Citrix Provisioning 2402 LTSR.
27 Aug 2025	Release of Citrix Provisioning 2402 LTSR CU3	See Citrix Provisioning 2402 LTSR.
07 Mar 2025	Release of Citrix Provisioning 2402 LTSR CU2	See Citrix Provisioning 2402 LTSR.
16 Oct 2024	Release of Citrix Provisioning 2402 LTSR CU1	See Citrix Provisioning 2402 LTSR.
15 Apr 2024	Initial release of Citrix Provisioning version 2402 LTSR	For a summary of new and improved features, see Citrix Provisioning 2402 LTSR