Citrix Provisioning 1808

Contents

What's new

September 6, 2018

This release includes improved performance with asynchronous I/O streaming, storage migration enhancements, SQL updates, support for Windows performance counters, and support for UEFI guest VMs for Nutanix AHV. See the fixed and known issues for additional information about this release of Citrix Provisioning.

> **Note:**
>
> Use the most recent version of the Citrix License Server for the latest features. If you are upgrading from an existing version to the newest version, the most recent version of the license server is available by using the product software. When you do not upgrade to the latest version of the license server, the product license enters the 30-day grace period. For more information, see Licensing.

Improved performance with asynchronous I/O streaming

A target device previously served incoming operating system storage requests by traversing through three different layers (RAM cache, VHDX file, and network streaming) sequentially to complete a request. This traversing leads to less than optimal performance due to the latency introduced when waiting for sub-IO completion, before submitting a new sub-IO request.

This release includes updates to the Citrix Provisioning target device that supports asynchronous IO in all three layers of the provisioning model: RAM cache, the VHDX file, and network streaming, effectively improving performance by adding asynchronous IO functionality.

> **Important:**
>
> This feature 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 IO:

- Private or maintenance mode
- Cache in device RAM with overflow on hard drive
- Cache on server persistent

By default, this asynchronous I/O feature is disabled. To enable it, apply a registry to Citrix Provisioning target device based on one of the following scenarios:

- For a new installation of Citrix Provisioning: Apply the registry update after finishing the installation of Citrix Provisioning on the target device and before running the Imaging Wizard.

- For a vDisk upgrading a target device to this version of Citrix Provisioning, apply the registry update when the vDisk is in *Private* or *Maintenance* mode.

> **Note:**
>
> Reboot the target device to apply the registry change.

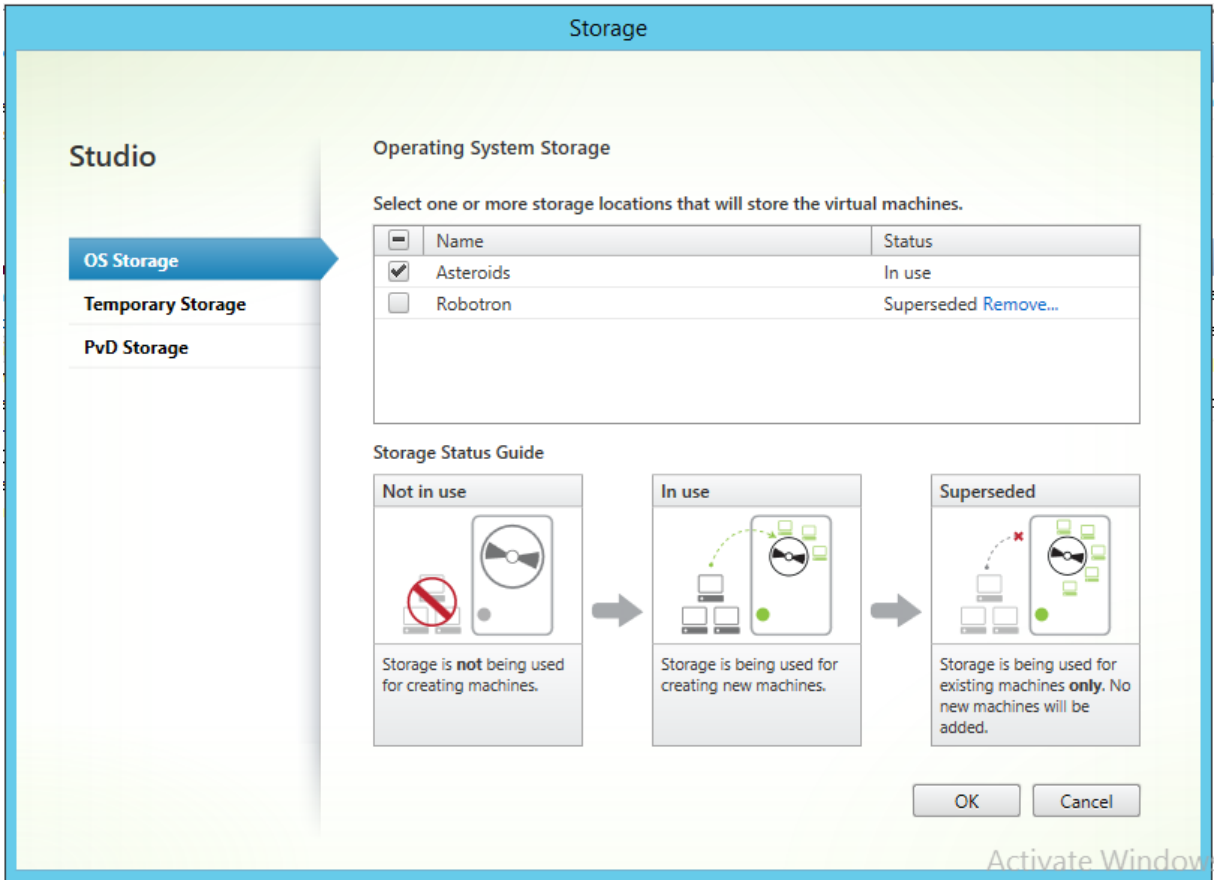
Apply the following registry change:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CVhdMp\Parameters]
“AsyncIO”=dword:00000001

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

Implementing UEFI guest VMs for Nutanix AHV hosts

This release of Citrix Provisioning allows you to implement a UEFI guest VM for Nutanix AHV hosts. The following prerequisites exist:

- The Citrix 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 should be 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 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, vDisk, and other elements. Choose **No** to shut down the target device, rather than rebooting it at the conclusion.
8. Set the VM to boot from the ISO boot and PXE boot the VM. Select one of the following boot options:
    - ISO boot – mount a BDM ISO created from the Provisioning Console. SSH into Nutanix Acropolis and run the following command: **acli vm.update_boot_device VM NAME disk_addr=CDROM BUS**. For example, acli vm.update_boot_device testVM disk_addr=ide.0; this example assumes that the CDROM is bus IDE 0.
    - Network boot - SSH into Nutanix Acropolis and run the following command: **acli vm.update_boot_device mac_addr= , acli vm.update_boot_device testVM mac_addr=52:54:00:2c:ff:03
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 vDisk 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 vDisk 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 Citrix Virtual Apps and Desktops Setup Wizard prompts you to create a cache disk.
15. Use the Citrix Virtual Apps and Desktops Set Up Wizard to provision UEFI provisioning target devices using the created vDisk.

SQL basic availability groups

Citrix Provisioning improves SQL functionality for 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:

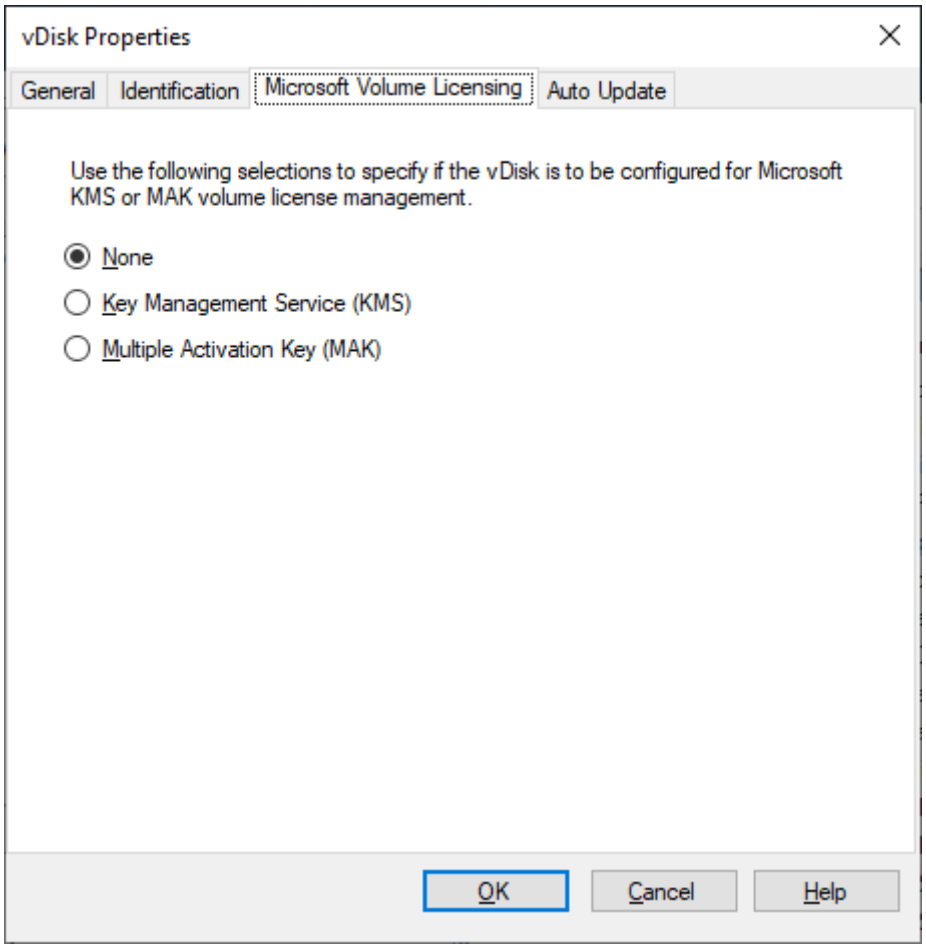
- Limit of two replicas (primary and secondary).
- No read access on secondary replica.
- No backups on secondary replica.
- No integrity checks on secondary replicas.
- Support for one availability database.
- Basic availability groups cannot be upgraded to advanced availability groups. The group must 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.

Active Directory-based activation

This release improves Active Directory functionality by updating how Microsoft Volume Licensing is configured for an individual vDisk. With this improvement you can specify that the vDisk uses no volume licensing.



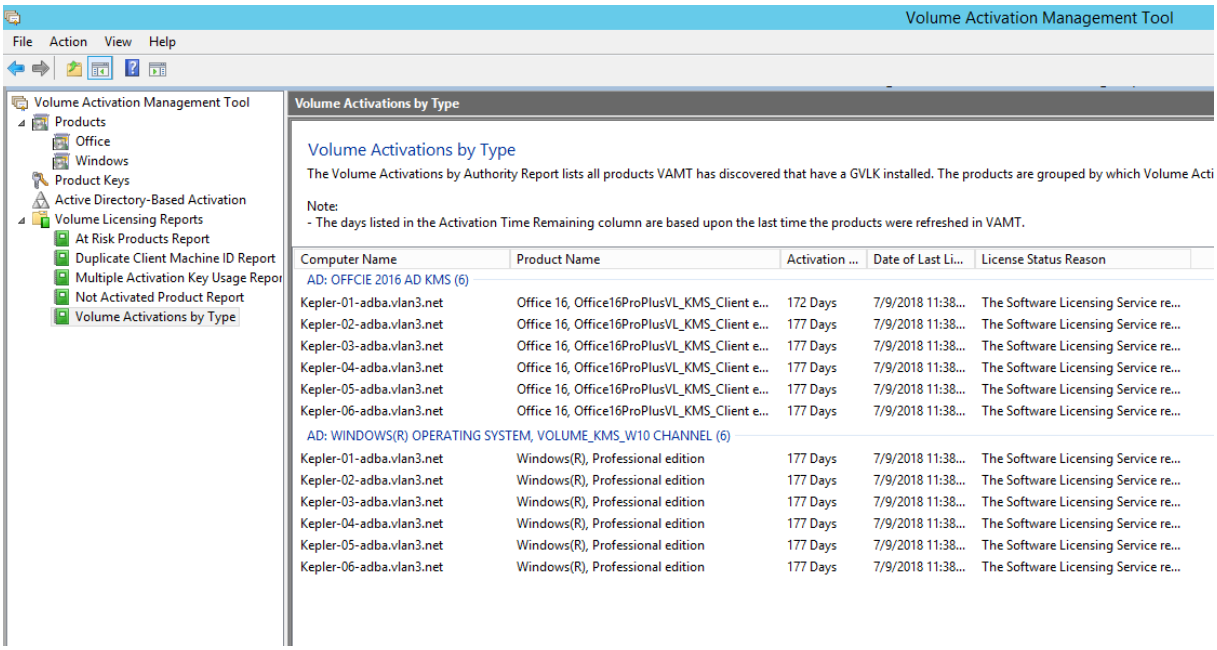
> **Note:**
>
> When using the Microsoft Volume Licensing for a vDisk, consider that Key Management Services (KMS), Multiple Activation Key (MAK) and Active Directory-based activation (ADBA) cannot be used together.

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 occurs although ADBA does not utilize CMID. ADBA, despite being similar to KMS, does not use CMID. Microsoft reuses KMS data when compiling CMID information. The image below illustrates a VAMT tool screen for ADBA. The Duplicate Client Machine ID report displays conflicts for duplicate CMID entries for those devices.

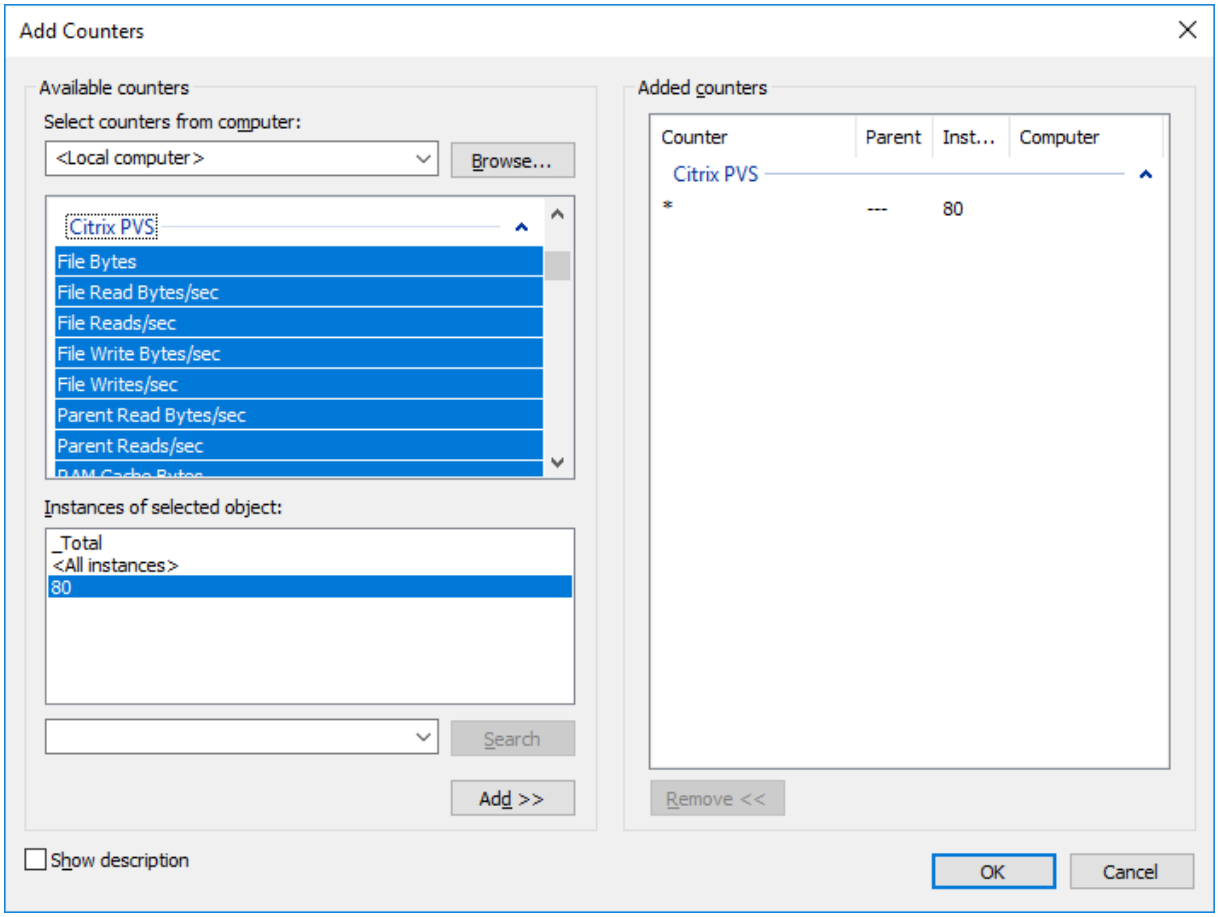


Support for Windows performance counters

Citrix Provisioning target devices now provide Windows performance counters for each storage tier:

- RAM cache
- VHDX file
- network streaming

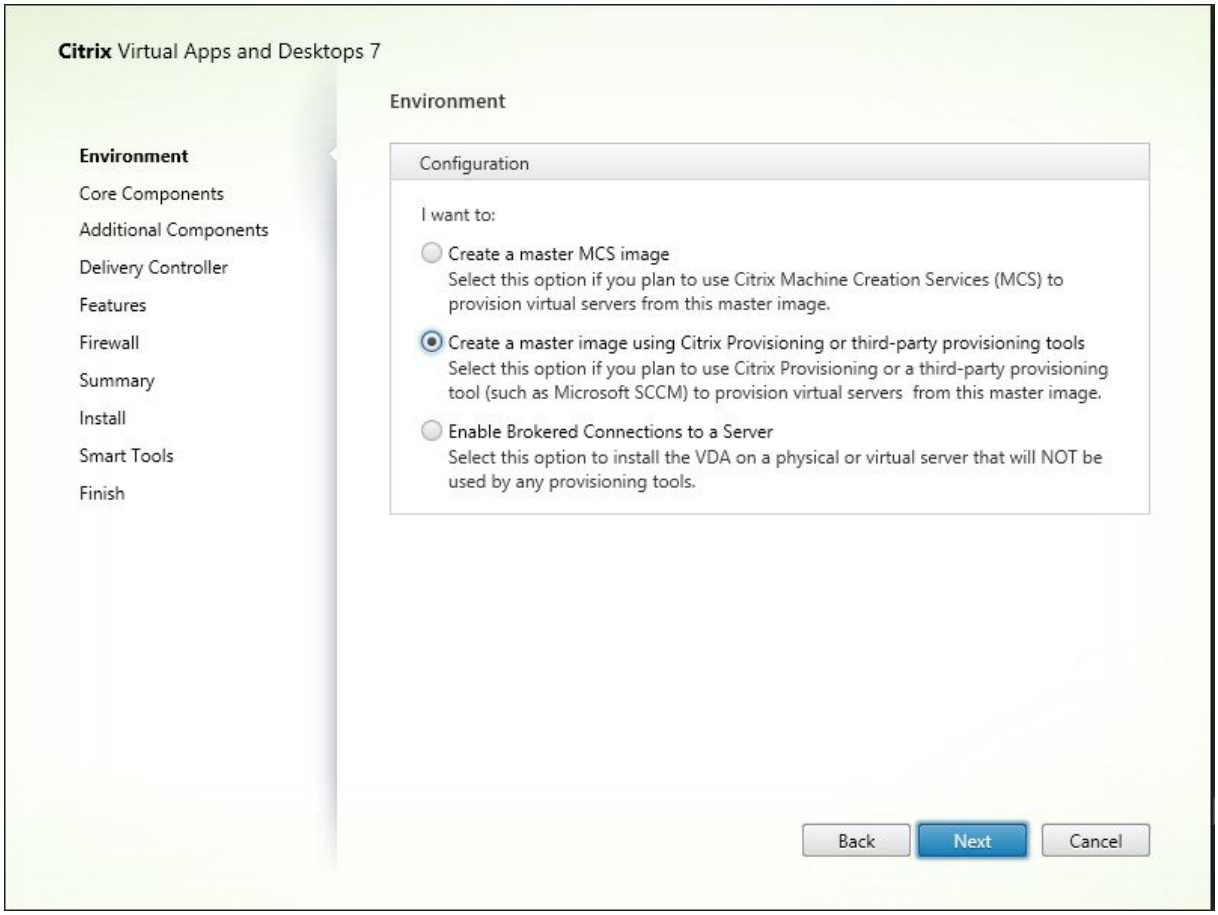
Using these performance counters, you can monitor target device streaming IOPS, bandwidth usage, current RAM usage, and VHDX file size.



VDA installer update for provisioned master images

The Citrix Virtual Apps and Desktops environment allows you to install the Virtual Delivery Agent (VDA) on a virtual master image. Use this feature if you are configuring Citrix Provisioning or third party tools to provision virtual servers from that master image.

> **Note:**
>
> When creating targets for Citrix Provisioning, select **Create a Master Image using PVS or 3rd Party Provisioning Tools**. When you select this option, Machine Creation Services (MCS), including MCS IO, is not installed.



How do I?

Use How Do I? pages in the Citrix Knowledge Center for additional information related to configuration, networking, antivirus, or hypervisor related procedures. These pages are purpose-built to help resolve problems arising from the use of Citrix Provisioning.

Fixed issues

August 30, 2018

Citrix Provisioning 1808 contains all fixes that were included in previously released versions 7 through 7.18, plus the following new fixes:

Server issues

- When an additional virtual hard disk (VHD) footer is assigned to a merged VHD, the file size of the merged base might increase. [#LC9837]

- When you create a merged base vDisk version, the MgmtDaemon.exe process might exit unexpectedly with an exception code 0xc0000005. [#LC9143]
- When you merge two or more vDisks at the same time, the MgmtDaemon.exe process might exit unexpectedly. [#LC9123]

Console issues

- On Citrix Provisioning 7.14 and later versions, the Configuration wizard might fail to configure a farm when you are not using Active Directory. The issue occurs when Citrix Provisioning is installed in a Workgroup environment. [#LC9844]
- After upgrading Citrix Virtual Apps and Desktops from Version 7.13 to Version 7.15 in certain Active Directory environments, the local users might not be able to log on to the Citrix Provisioning Console. A timeout error message appears. [#LC9542]

Known issues

October 5, 2018

The following issues are known at this release:

- Provisioning Services UEFI target devices do not support the **List local hard disk in boot menu** option. If you select this option in the boot menu, the system does not boot to hard disk for UEFI target devices. Instead, the system shows the boot menu again after timing out.
- When using the Citrix Cloud feature, consider the following:
  - To install the remote PowerShell SDK on the Provisioning server, you must uninstall the 5 Citrix Virtual Apps and Desktop snap-ins from the server, then install the remote PowerShell SDK.
  - Once a Console is installed with the remote PowerShell SDK and is used for provisioning, it no longer functions with on-premise Citrix Virtual Apps and Desktops.
  - In the Citrix Virtual Apps and Desktops Setup Wizard, enter the **IP address** for the Citrix Cloud connector when it prompts for the Citrix Virtual Apps and Desktops Controller Address.
- Before upgrading from version 7.17 to this version of Citrix Provisioning, you must manually uninstall CDF on the Provisioning Server, Console, and target devices.
- For Windows 10 1709, you must apply the OS update KB4093105, or later, before installing Citrix Provisioning components.
- In the Provisioning Console, the Citrix Virtual Apps and Desktops Setup Wizard cannot be used to connect twice in a row. Once the Wizard tries to connect to the Cloud Delivery controller once, regardless of connection success or failure, you must exit and close the Provisioning Console.
- Citrix Provisioning supports Windows 10 Fall Creator v1709 with the following known issues:

  - Windows 10 32 bit v1709 cannot boot from a vDisk in private image mode. [LCM-3224]
- After performing a silent install of a Citrix Provisioning client, subsequent upgrades using the Upgrade Wizard fail because the client fails to reboot. [#PVS-2264]
- Existing Citrix Provisioning target devices cannot be added to an existing Citrix Virtual Apps and Desktop catalog using the Machine Creation Services catalog in Studio. However, new target devices created using the Citrix Virtual Apps and Desktop Setup Wizard can be added to the existing catalog from the Provisioning server. [#DNA-53806]
- When using the Citrix Provisioning 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". This 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. [#PVS-1126]
- The Citrix Virtual Apps and Desktop Setup Wizard creates targets then boots them to format the cache drive. This process occurs quickly. Sometimes, a VDA may reach a state where it fails to shut down correctly because it's initializing while the Citrix Provisioning Device Service simultaneously finishes formatting the cache drive then shuts down the target. To resolve this issue, in the vDisk registry key, HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices, create a DWORD called "RebootDelaySec". Set an arbitrary value, delay-to-shutdown, in seconds using a decimal value. [#HDX-14474]
- The MCS IO driver may cause a system to crash. To resolve this issue, Citrix recommends disabling the driver in Studio. [#PMCS-2941]
- Windows 10 v1803 target devices with vDisk cache type set to **Cache in device RAM** may crash when booting. [#PVS-3634]

Deprecation

August 29, 2018

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 may 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.

- **Printer management:** Labeled **Enable printer management** in the vDisk Properties screen. This item was announced in version 7.12.
- **In the BDM Media Properties section of the Boot Device Management screen, the term *BDM Secure Boot*:** This item was announced in version 7.12.

  The alternative is as follows: The **Protect SDB** parameter will replace **BDM Secure boot**. This new paramter will represent the same level of functionality previously provided by the BDM Secure Boot option. To use this feature:

  1. In the Boot Device Management screen, select the **Protect SBD** checkbox.
  2. Optionally select **Generate random password** (make Media Write-Once), then enter the password and confirmation.
  3. Click **Burn** to create the bootable device.
- **The vDisk Properties screen will be updated to remove the following options from the Cache Type field:**

  – Cache on hard disk. This option will be removed from the list of available parameters on the vDisk Properties screen; this option can still be configured using an API.
  – Cache on hard disk persisted. The cache on hard disk parameter will be removed due to lack of ASLR support.

  This item was announced in version 7.12. As an alternative, use one of the other available options.

System requirements and compatibility

September 11, 2018

The system requirements in this article were valid when this Citrix Provisioning version was released; updates are made periodically. System requirements components not covered here (such as StoreFront, host systems, and Citrix Receivers and plug-ins) are described in their respective documentation.

> **Important:**
>
> Review the pre-installation 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

The following databases are supported: Microsoft SQL Server 2008 SP3 through 2016 (x86, x64, and Express editions).

Database clustering is supported.

> **Note:**
>
> Refer to Supported Databases for Citrix Virtual Apps and Desktop 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 Desktop installation media. You should always 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. You must 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:** The following operating systems are supported: Windows Server 2016, Windows Server 2012 R2; Standard, Essential, and Datacenter editions, Windows Server 2008 R2 and Windows Server 2008 R2 SP1; Standard, Enterprise, and Datacenter editions. 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.
- **Storage:** Disk storage management is important because a Provisioning Server can have many vDisks stored on it, and each disk can be several gigabytes in size. Imporove 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 vDisk. Additional 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 vDisk in Private Image mode (vDisks in Private Image mode should be backed up daily).
  - **Standard Image Mode** – the number of target devices using a vDisk in Standard Image mode. Best practice is to include making a copy of every vDisk created. Minimum common storage sizes: 250 MB for the database, 5 GB on a clean Windows system, 15 GB per vDisk for Vista Class images (estimated).
- **Network adaptor:** Static IP, Minimum 100 MB Ethernet, 1 GB Ethernet preferred; Dual 1 GB Ethernet for more than 250 target devices. Two NICs often perform better than a single dual-ported NIC.
- **Citrix Provisioning dependencies:** The Provisioning Server install program requires Microsoft NET 4.7.1 and Windows PowerShell 3.0.

Network

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) in order to communicate with each other using the Messaging Manager. 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 (HA), all Provisioning Servers selected as failover servers must reside within the same site. HA 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) in order 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, target device to Citrix Provisioning communication cannot be configured.

  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

- **Console communication:** The SOAP Server is used when accessing the 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`.

TFTP

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

  Default port (TFTP): 69

TSB

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

  Default port (UDP): 6969

  Port Fast: Port Fast must be enabled

  Network card: PXE 0.99j, PXE 2.1 or later

  Addressing: DHCP

Target device

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

> **Tip:**
>
> When using the vDisk Imaging Wizard for a target device, you may encounter problems related to some Microsoft components which are not installed. For example, operating systems that do not have Microsoft Visual C++ may 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.

In order to have a single vDisk, all target devices must have certain similarities to ensure that the OS has all of the drivers it requires to run properly. The three key components that should be consistent are the motherboard, network card, or video card.

If NIC teaming is desired, the Microsoft NIC teaming driver or OEM NIC teaming software should be installed and configured before you install the target device software.

> **Tip:**
>
> The Unified Extensible Firmware Interface (UEFI) is supported, however, secure boot is only supported using a Hyper-V 2016's Secure Boot VM that uses the Microsoft UEFI Certificate Authority template.

Target devices are identified by the operating system running on the device.

> **Note:**
>
> Dual boot vDisk images are not supported.

The operating systems identified in the list below are supported for target devices:

- **Operating System:** Windows 10 (32 or 64-bit); all editions. Note the following:
  - Support for the publicly available version at the time of the release. Windows 8.1 (32 or 64-bit); all editions. Windows 7 SP1 (32 or 64-bit); Enterprise, Professional, Ultimate.
  - The Ultimate edition of Windows 7 is supported only in *Private Image mode*. Windows Server 2016 Windows Server 2012 R2; Standard, Essential, and Datacenter editions; Windows Server 2008 R2 and Windows Server 2008 R2 SP1; Standard, Datacenter, and Enterprise editions.
  - Ensure that all Windows updates are current before installing Citrix Provisioning components. In some cases, you may have to install numerous updates. Citrix recommends that you reboot after installing all Windows updates.
- **Gen 2 VMs:** For Citrix Provisioning support for Gen 2 VMs in a Virtual Apps and Desktops environment, the following operating systems are supported:
  - Windows 2016
  - Windows 10 (with or without secure boot)
  - Windows Server 2016, Windows Server 2012 R2; Standard, Essential, and Datacenter editions
- **Linux streaming:** For Linux streaming, the following operating systems are supported: Ubuntu desktop versions 16.04, 16.04.1 and 16.04.2 (with the 4.4.x kernel)
  - When using these distributions for Linux streaming, consider that the Citrix Provisioning installer requires that the Linux kernel package version is greater than or equal to version 4.4.0.53. The installer automatically provides the correct version during the installation

process. RedHat Enterprise Linux Server 7.2, 7.3; CentOS 7.2, 7.3; SUSE Linux Enterprise Server (SLES) 12.1, 12.2 are supported.
  - The default kernel used for Ubuntu 16.04.2 is version 4.8; this kernel version is not currently supported.
  - If you are using Linux streaming functionality, no new installation packages are provided at this release. Use the Citrix Provisioning 7.15 Linux DEB/RPM package. For example, after downloading the Citrix Provisioning 1808 ISO, the target software for CentOS/Red Hat is pvs_RED_HAT_7.15_18089_x86_64.rpm.

- **Additional dependencies:** .NET 4.7.1 (default)
- **Microsoft licensing:** Consider the following when using Microsoft licensing keys with target devices:
  - Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2008R2 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 vDisk image when the Imaging Wizard is run on the Master target device. Volume licensing is configured for the vDisk file on the Microsoft Volume Licensing tab, which is available from the **Console vDisk File Properties** dialog.
  - In order 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.

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

Console

Processor: Minimum 1 GHz, 2 GHz preferred

Memory: Minimum 1 GB, 2 GB preferred

Hard disk: Minimum 500 MB

Operating systems:

- Windows Server 2016
- Windows Server 2012 R2; Standard, Essential, and Datacenter editions

- Windows Server 2008 R2 and Windows Server 2008 R2 SP1 Standard, Datacenter, and Enterprise editions
- Windows 10 (32- or 64-bit)
- Windows 8.1 (32- or 64-bit); all editions
- Windows 8 (32- or 64-bit); all editions
- Windows 7 (32- or 64-bit)
- **Additional dependencies:** MMC 3.0, Microsoft .NET 4.7.1, 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; the version levels must be the same. In addition:

- One or more configured Citrix Virtual Apps and Desktops hosts with identical templates must exist.
- You must create a Device Collection in the Citrix Provisioning site.
- The vDisk assigned to each VM must be in standard image mode.

Additional requirements include:

Permissions:

Consider the following:

- A Citrix Virtual Apps and Desktops controller must exist with permissions for the current user.
- vCenter, 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. This user 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 new accounts in the Console, the user needs the Active Directory Create Accounts permission. To use existing accounts, Active Directory accounts have to already 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 (eliminating the need to boot using PXE) and an unformatted write cache disk is automatically attached and formatted on first boot.
- When updating the Virtual Desktop Agent (VDA) on the vDisk image, you must also 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. This is the same formatting used by the Active Directory Users and Computers MMC when exporting the contents of an organizational unit. If you are using Personal vDisks with Citrix Virtual Apps and Desktops, the SOAP Server user account must have Citrix Virtual Apps and Desktops full administrator privileges.

SCVMM:

- SCVMM servers require that PowerShell 2.0 is installed and configured for the number of planned connections.
- The number of required connections for an SCVMM server should be 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 work with 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.

Additional requirements:

- If you are running a vCenter server on alternate ports, the following registry modifications must be made in order to connect to it using Citrix Provisioning: **Create a new key** HKLM\Software\Citrix\ProvisioningServices\PlatformEsx - **Create a new 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, and therefore changes it in accordance with the virtual machine network in the Domain Controller. This 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 Set Up Wizard is used with SCVMM, both the first legacy and the synthetic NICs' network change according to the network resource 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 Desktop agents are supported on VMs. For details, refer to 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 vDisk in Standard Image mode must exist, to be associated with the selected VM template.

Addtional requirements are described below:

Template VM:

- **Boot order:** Network/PXE must be 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 should be added to a provisioning **SiteAdmin group** or above.
- If you are using Active Directory, when creating new 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 vDisk Update Management

ESD server requirements include:

- **WSUS server:** 3.0 SP2
- **SCCM:** SSCM 2016, SCCM 2012 R2, SCCM 2012 SP1, SCCM 2012

Hypervisor

For a list of supported hypervisors, refer to Citrix Virtual Apps and Desktops and Citrix Provisioning Hypervisor support.

Additional requirements for each supported hypervisor are described in the following sections:

Citrix Hypervisor 5.6 and newer

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

Nutanix Acropolis

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

- Linux VMs
- BDM partition
- UEFI

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

> **Important:**
>
> An Acropolis hypervisor (AHV) plugin from Nutanix that supports Citrix Provisioning is required. Download this plugin from the Nutanix support site. Refer to the Nutanix documentation site for installation information.

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

Consider the following when configuring this type of hypervisor:

- VMM 2012, 2012 SP1, and 2012 R2 are significantly 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 vDisk 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.
  - To use BDM to boot a VM that uses a personal vDisk and write cache, create a VM with three hard disk drives.
- To do the 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. This is because VMM uses the last legacy NIC and the Citrix Virtual Apps and Desktops Set Up 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 Set Up Wizard, you may find that the targets are created but are not bootable with the error Device not found in the Citrix Provisioning database. This usual 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 4.1 and newer

- **Supported Citrix Provisioning PXE NIC:** ESX 4.x – E1000, ESX 5.0 and newer – VMXNET3
- **Template VM and the master 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:**
  - vCenter 5.5 defaults to virtual machine version 8, which is for ESX 5.0.
  - The virtual machine version must be changed before OS installation.
  - The template and the master VM must have the same virtual machine version.
- **Windows 7 and Windows 2008 R2 with VMXNET NICs:** - Windows 7 and Windows 2008 R2 without service packs: Install the Microsoft iSCSI hotfix http://support.microsoft.com/kb/2344941 and restart the VM before installing Citrix Provisioning target device software.
  - Windows 7 and Windows 2008 R2 with Service Pack 1: Install Microsoft iSCSI hotfix http://support.microsoft.com/kb/2550978 and restart the VM before installing Citrix Provisioning target device software.
- **ESX:**
  - For ESX 5.0 only, the Interrupt Safe Mode must be enabled on the Citrix Provisioning bootstrap. Otherwise, the VM displays a partial MAC address during reboot
  - With ESX 5.5, a VM created using the Web client defaults to virtual hardware version 10 (ESX 5.5) and a VM created using the vSphere client defaults to version 8 (ESX 5.0)
  - When creating a new ESXi 5.5 template using the vSphere web client, you can only create hardware version 10 templates. Be sure to modify the template CD/DVD drive virtual mode from SATA to IDE. Remove the SATA controller if you are planning to use the VMXNet3 driver. This will ensure that the template is compatible with the Citrix Virtual Apps and Desktops Setup Wizard, which requires the drives that are created for the target to be attached using the SCSI driver.
  - When using multiple NICs in ESX VM, be aware that the order of the NICs in the VM's properties, BIOS, and OS may differ. Keep this in mind when making your choices for the streaming NIC. This should be 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 will be that of the vCenter system. Do not enter the address used by the web client.

Linux streaming

> **Important:**
>
> If you are using Linux streaming functionality, no new installation packages are provided at this release. Use the Citrix Provisioning 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.

Distributions:

- Ubuntu 16.04, 16.04.01 and 16.04.02 with the 4.4.x kernel.
  - When using these distributions for Linux streaming, consider that the Citrix Provisioning installer requires that the Linux kernel package version is greater than or equal to version 4.4.0.53. The Citrix Provisioning installer automatically provides the correct version during the installation process.
  - The following distributions are supported: RedHat Enterprise Linux Server 7.2, 7.3; CentOS 7.2, 7.3; SUSE Linux Enterprise Server (SLES) 12.1, 12.2.
- **Hypervisors:** XenServer, ESX
- **Image management:** Versioning.

  > **Note:**
  >
  > Reverse imaging is not necessary with Linux.
- **Caching:** All cache modes supported.
  - Refer to the Managing vDisks article for more information on supported cache types.
  - Once the write cache disk has been formatted, the Linux client will not shut down. Instead, it automatically begins using the cache disk.
  - *Cache on device hard disk* and *Cache in device RAM with overflow on hard disk* both use the Linux file system caching mode.

> **Important:**
>
> Linux streaming functionality works with the latest version of Citrix Provisioning in conjunction with corresponding versions of Citrix Virtual Apps and Desktops.

Licensing

August 30, 2018

The Citrix License Server must be installed on a server within the farm that is able to communicate with all Citrix Provisioning Servers within the farm. You need one license server per Citrix Provisioning farm.

> **Important:**
>
> Provisioning Servers must be connected to the license server to operate successfully, it will not work out-of-the-box. You must 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.

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 vDisk volume licensing, see Configuring a vDisk for Microsoft Volume Licensing.

Licensing grace periods

There are two types of grace period:

- **Out-of-box grace period** 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, regardless of whether it is valid or invalid.
- **License server connectivity outage grace period** 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 grace period, administrators are notified through warning messages in the Provisioning Console.

When a grace period expires, all target devices are shut down.

> **Note:**
>
> When you upgrade an existing environment to the newest version of Citrix Provisioning, you must also upgrade to the latest version of the licensing server or the product license will enter a 30-day

> grace period and new product features will be unavailable.

Installing the License Server

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

> **Note:**
>
> If Citrix Provisioning is installed after the license server or if new licenses are added, you must restart the Stream Service.

New license type for Citrix Cloud

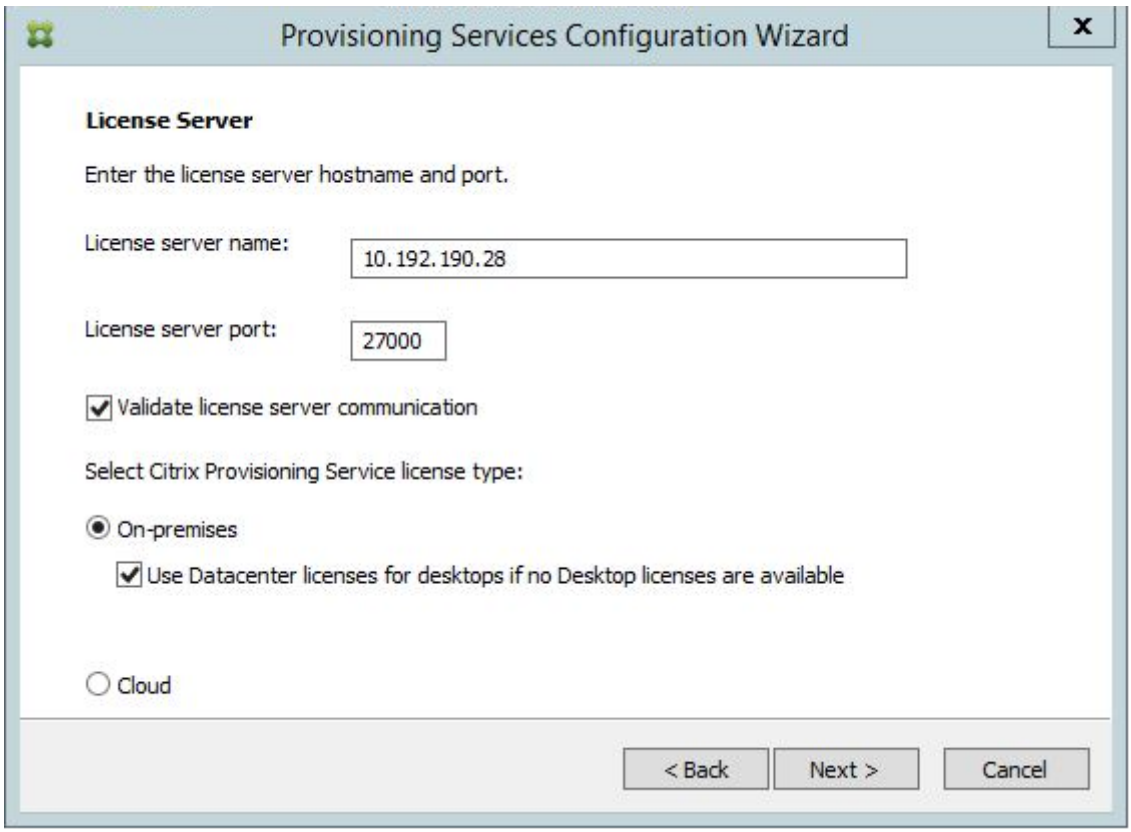
This release introduces a new license type (PVS_CCLD_CCS) providing support for XenApp and XenDesktop Service in Citrix Cloud. This license type is applicable to both desktop and server operating systems that service Citrix Provisioning target devices. It replaces the existing on-premises Provisioning Services license for Desktops and PVS for data centers.

> **Note:**
>
> This new Citrix Cloud license type replaces the existing on-premises Citrix Provisioning license for Desktops and provisioning for data centers; it possesses the same license acquiring precedence as the on-premises licenses when bundling Citrix licenses.
>
> The on-premises trade-up feature does not apply to Citrix Cloud licenses. Each Citrix Provisioning target device checks out a single Citrix Cloud license regardless of the operating system type, for example, a data center or desktop.

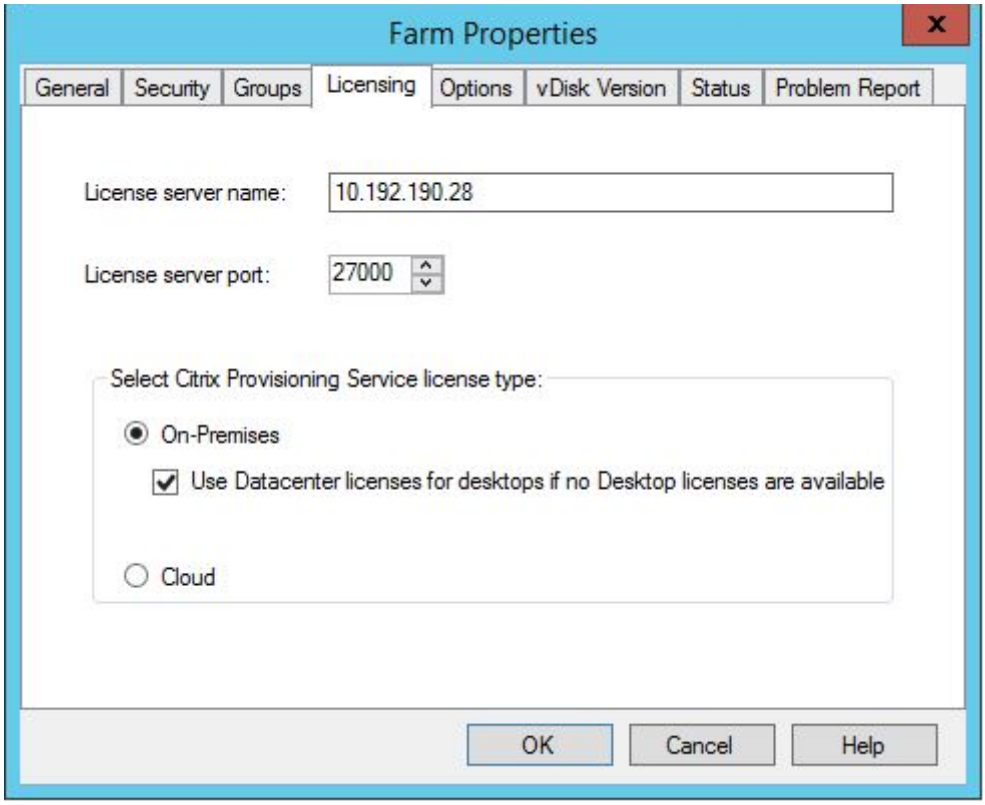
Citrix Provisioning license options for Citrix Cloud are controlled by the options associated with Citrix Provisioning Services license types, *on-premises* or *Citrix Cloud*. Using a license server with Citrix Provisioning, Citrix Cloud licenses will be consumed if the Cloud option is selected during initial setup. Conversely, an on-premises license is consumed if **On-premises** is selected when setting up Citrix Provisioning.

> **Important:**
>
> You must restart the Citrix Provisioning Stream Service whenever changes are made to licensing options, for example, when changing from a Citrix Cloud license to an on-premises licensing schema.

Use the Citrix Provisioning Configuration Wizard to specify a Cloud license. In the License Server screen, click the **Cloud** radio button, then click **Next** to continue with the configuration process:



You can alternately view or change the license type in the Farm Properties screen. In the Licensing tab, select the appropriate license type; click **Cloud** then click **OK:**



> **Note:**
>
> The on-premises trade-up feature does not apply to Citrix Cloud licenses. Each Citrix Provisioning target device checks out a single Citrix Cloud license regardless of the operating system type, for example, a data center or desktop.

Configuring a vDisk for Microsoft Volume Licensing

August 30, 2018

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

> **Note:**
>
> The MCLI and SOAP Server command-line interfaces can also be used to configure Microsoft volume licensing using the following procedure:

1. Select the vDisk in the 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 keys with Citrix Provisioning.

> **Note:**
>
> Support for KMS licensing requires that the SOAP Server user account is a domain user with the right to **perform volume maintenance task**. This 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 would have this right.

KMS volume licensing utilizes a centralized activation server. This server runs in the datacenter, 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. You must change the vDisk mode from **Private Image Mode** to **Shared Image Mode**. Do this 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 include:

- Enabling KMS licensing on the created vDisk. Select the KMS menu option on the Microsoft Volume Licensing tab when running the Imaging Wizard (refer to 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. The operating system needs to be reinstalled 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 on 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.

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 base disk preparation once, repeat the base disk preparation using the following procedure:
   a) In the 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.

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, which 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 network access to the internet. Citrix Provisioning applies this proxy activation mechanism for Standard Image mode vDisks that have MAK licensing mode selected when creating the vDisk.

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) available at: http://www.microsoft.com/en-US/download/details.aspx?id=39982. Upon first execution of 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 – the OS is earlier 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.
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 Provisioning Services 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.c
to C:\Users\<Provisioning Services soap/stream services user>\AppData\Roaming\Microsoft\VAMT\VAMT.cor

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 http://technet.microsoft.com/en-us/library/hh849812(v=wps.620).aspx for more information.
    b) WinRM quickconfig.
    c) Enable-WSManCredSSP -Role Client -DelegateComputer <this server fqdn> -Force
    d) Enable-WSManCredSSP -Role Server –Force.
6. Configure Windows firewall on the client for VAMT 3.1 – see http://technet.microsoft.com/en-us/library/hh825136.aspx 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 should be set before attempting to activate target devices.

Note: For information on using the command-line interfaces, refer to 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 that require 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 and may result in some target devices not being activated. The **Status column** indicates if a target device is being activated (Activating) or the activation failed (Failed). If all target devices were activated successfully, click OK to close the dialog. If one or more target devices were not selected for activation, 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 additional vDisks to the target device, without removing any, then set the default booting vDisk accordingly.
- Assign additional 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 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.
- Use of Auto Update to deploy a new vDisk, from a different OS install than the previous vDisk, 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

August 8, 2018

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 often surpassed by operational costs.

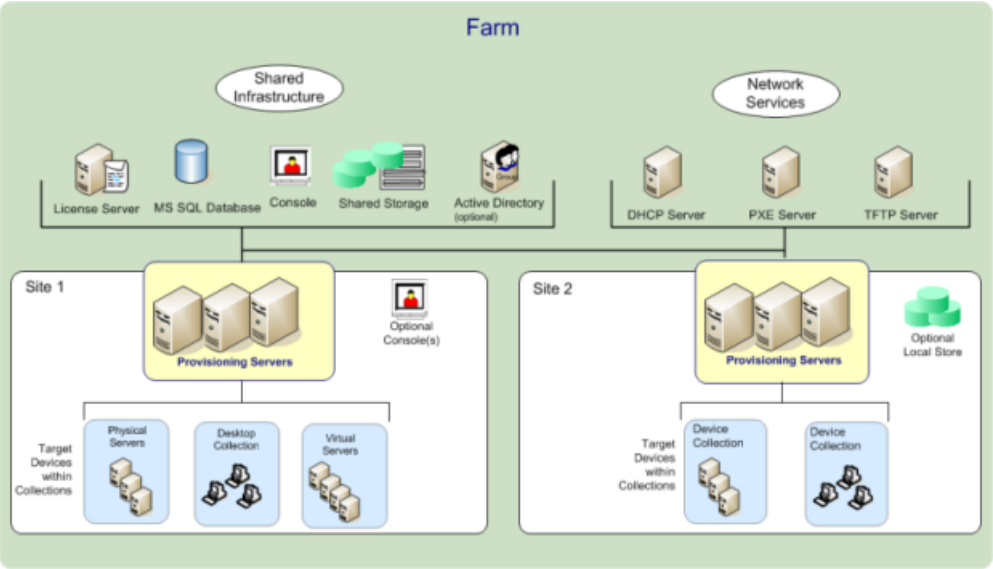
Citrix Provisioning takes a very different approach from traditional imaging solutions by fundamentally changing the relationship between hardware and the software that runs on it. By streaming a single shared disk image (vDisk) rather than copying images to individual machines, Citrix Provisioning enables organizations to reduce the number of disk images that they manage, even as the number of machines continues to grow, simultaneously providing the efficiencies of a centralized management with the benefits of distributed processing.

In addition, because machines are streaming disk data dynamically and in real time from a single shared image, machine image consistency is ensured, while 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 vDisk can be configured in *Standard Image mode*. A vDisk in 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 storage that would be required. The vDisk is in read-only format and the image can not be changed by target devices.

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



Benefits of XenApp and other server farm administrators

If you manage a pool of servers that work as a farm, such as Citrix Virtual App servers or web servers, 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 as soon as a server is built with the master image, you now must patch the individual server along with all of the others. Rolling patches out to individual servers in your farm is not only inefficient, but it can also be unreliable. Patches often fail on an individual server and you may not realize you have a problem until users start complaining or the server has an outage. Once that happens, getting the server back into sync with the rest of the farm can be challenging and sometimes it can require a full re-imaging 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 boot-up. Server build consistency is assured because all your servers are using a single shared copy of the disk image. If a server becomes corrupted, simply reboot it and it's instantly back to the known good state of your master image. Up-

grades are extremely fast. Once you have your updated image ready for production you simply 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. Just as importantly, roll-backs can be done in the same manner so problems with new images will not take your servers or your users out of commission for an extended period of time.

Benefits for desktop administrators

As part of Citrix Virtual Apps and Desktops, desktop administrators have the ability to 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 consolidation and simplified management needs of IT, deploying it also requires deployment of supporting infrastructure. Without Citrix Provisioning, storage costs can put desktop virtualization out of the budget. With Provisioning Services, 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 specifically tailored to meet the performance, security and flexibility requirements of each individual user.

Not all desktop applications can be 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 datacenter and streamed out to physical desktops on demand. This model works particularly well for standardized desktops such as those in lab and training 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 re-provisioned in real time from a single shared-disk image. This 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 can be used for runtime data caching or, in some scenarios, removed from the system entirely, which reduces power usage, system failure rates, and security risks.

The Citrix Provisioning infrastructure is based on software-streaming technology. After installing and configuring Citrix Provisioning components, a vDisk is created from a device’s hard drive by taking a

snapshot of the OS and application image, and then storing that image as a vDisk file on the network. The device that is used during this process is referred to as a master target device. The devices that use those vDisks are called target devices.

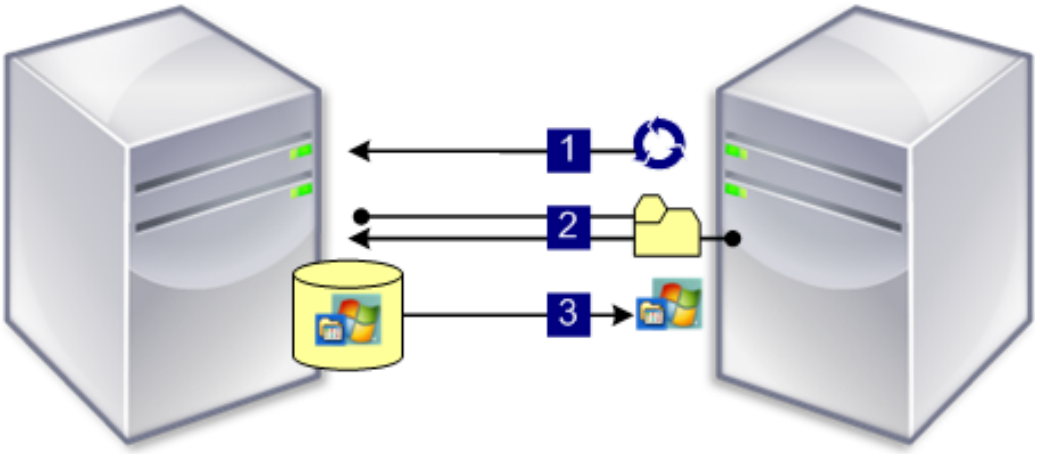
A vDisk may exist on:

- a Provisioning Server
- a file share
- a storage system that can communicate with the Provisioning Server with iSCI, 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 vDisk is located, then mounted on the Provisioning Server.



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

Instead of immediately pulling all the vDisk 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 completely new operating system and set of software in the time it takes to reboot, without requiring a visit to a workstation. This approach dramatically decreases the amount of network bandwidth required by traditional disk imaging tools, making it possible to support a larger number of target devices on your network without impacting overall network performance.

Components

August 29, 2018

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 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. Only one database can exist within a farm and all Provisioning Servers in that farm must be able to communicate with that database. You may 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 Provisioning Server.

Console

The 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 Provisioning Server added to that farm.

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

The Console does not need to be directly associated with the farm because remote administration is supported on any Console that can communicate with that farm's network.

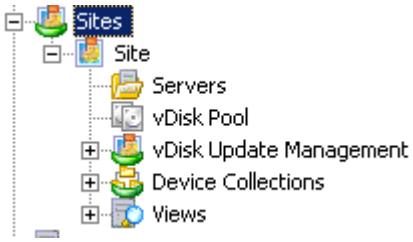
Stores

A farm contains one or more stores. A store is a logical name for a physical or virtual vDisk 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:



Provisioning servers

A 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 may get the vDisk 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.

vDisks

vDisks exist as disk image files on a Provisioning Server or on a shared storage device. A vDisk consists of a .vhdx base image file, any associated properties files (.pvp), and if applicable, a chain of referenced VHD differencing disks (.avhdx).

vDisks are assigned to target devices. Target devices boot from and stream software from an assigned vDisk image.

vDisk pools

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

vDisk update management

The vDisk Update Management feature is used to configure the automation of vDisk updates using virtual machines. Automated vDisk 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.

vDisk modes

vDisk images are configured for Private Image mode or Standard Image mode. Consider the following when using vDisk images:

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

vDisk chain

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

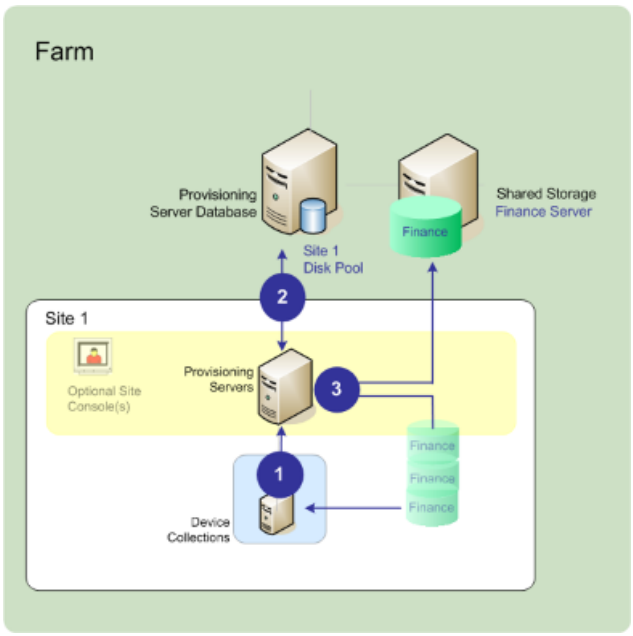
Each time a vDisk is updated, a new version of the VHDX differencing disk can be created and the file name is numerically incremented, as shown in the following table:

vDisk image	VHDX Filename
Base Image	win7dev.avhdx

vDisk image	VHDX Filename
Version 1	win7dev.1.avhdx
Version 2	win7dev.2.avhdx
…	…
Version N	win7dev.**N**.avhdx

Booting a vDisk

The following image shows the method used to locate and boot from a vDisk 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 vDisk pool for vDisk information, which includes identifying the Provisioning Servers providing the vDisk to the target device. The server also verifies the path information the server uses to get to the vDisk. In this example, the vDisk shows that only one Provisioning Server in this site can provide the target device with the vDisk and that the vDisk physically resides on the Finance Server (shared storage at the farm level.
3. The Provisioning Server locates the vDisk on Finance Server, then streams that vDisk, on demand, to the target device.

vDisk examples

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

Example one

The physical vDisk for Windows 10 resides on a 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 vDisk is: C:\vDisks\

Example two

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

Store name (logical name): FinancevDisks

Physical path to the vDisk 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 vDisk on the network. A device collection could 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 can represent a physical location, such as a building, or a user type. A target device can be a member of any number of views, although it can be 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

August 27, 2018

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 vDisk file in the database and then images that file without having to physically go to a 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 Provisioning Services 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, creates, and associates target devices to those VMs, assigns a vDisk 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 vDisk image all the VMs.
- Virtual Host Connection Wizard – Adds new virtual host connections to the vDisk Update Manager.
- Managed vDisk Setup Wizard – Adds new managed vDisks to the vDisk Update Manager.
- Update Task Wizard – Configures a new update task for use with vDisk 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. These utilities are 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

August 27, 2018

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 may have 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 Provisioning Servers, site properties, target devices, device collections, vDisks, vDisk pools, and local vDisk stores. 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 vDisk properties (read-only) and assigning or removing vDisks from a device. They 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), boot or shut down target devices, and send messages to target devices within a device collection to which they have privileges.

Collections

August 27, 2018

Device collections provide the ability 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 could represent a physical location, a subnet range, or a logical grouping of target devices. For example, a collection could consist of all target devices that use a particular vDisk image,

and that target device collection might consist of maintenance, test, and production devices. Alternatively, three device collections could exist for a particular vDisk; one consisting of production devices, one consisting of test machines, and another consisting of maintenance machines. In the proceeding examples, all of the devices in a given collection are assigned to the same vDisk.

Depending on a sites preference, another collection use case might include the consolidation of test and/or maintenance devices into a single device collection, and then managing vDisk 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 vDisk.

Device collections are created and managed by farm administrators, or site administrators that have security privileges to that site, or device administrators that have security privileges to that collection.

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 allowing you to view or make modifications to 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

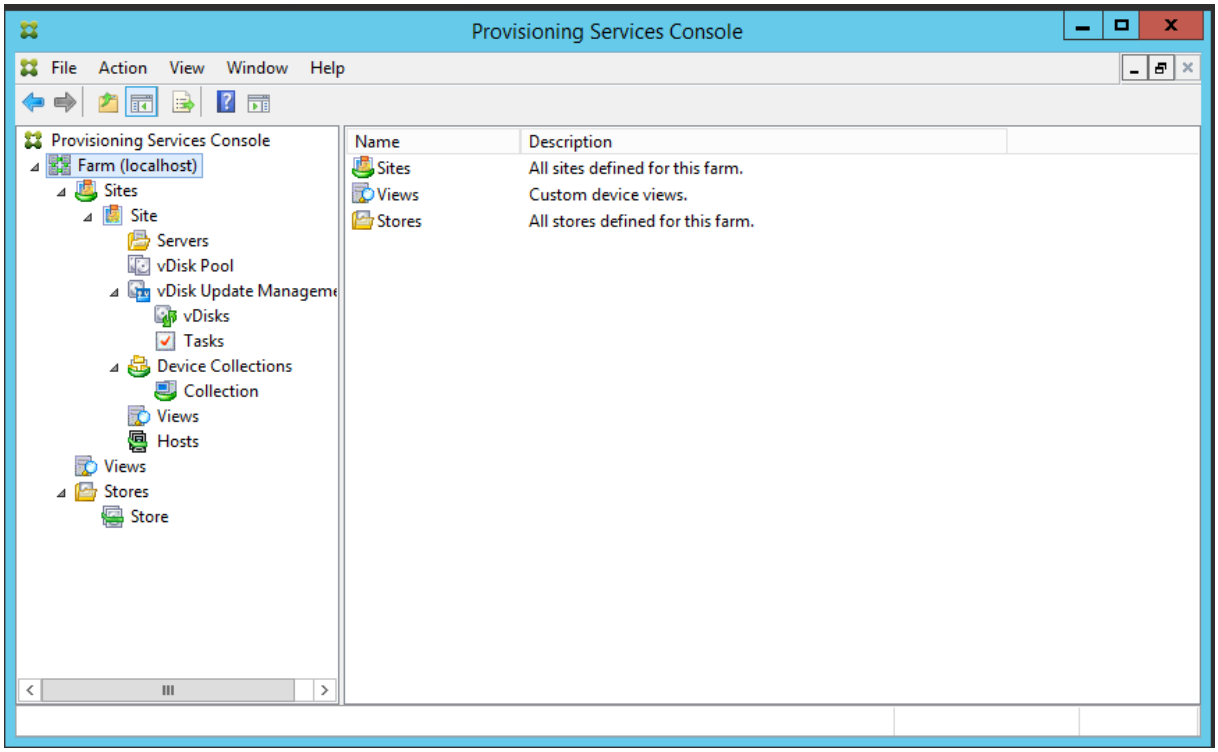
August 27, 2018

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

On the main Console window, you can perform tasks when setting up, modifying, tracking, deleting, and defining the relationships among vDisks, target devices, and Provisioning Servers within your network.



Using the Console tree

The tree is located in the left pane of the **Console** window. The tree shows a hierarchical view of your network environment and managed objects within your network. What displays in the Details view 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 vDisk pool, device collections, and views. The site-level tree is organized as follows:

- Site

- Servers
- Device Collections
- vDisk Pool
- vDisk 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

August 9, 2018

Before installing and configuring Citrix Provisioning software and components from the product CD-ROM or from the download site, you should 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 Provisioning Services components. In some cases, you may need to install numerous updates; Citrix recommends that you reboot after installing all Windows updates.
>
> **Tip:**
>
> If you are using Linux streaming functionality, no new installation packages are provided at this release. Use the Citrix Provisioning 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.

Provisioning Services 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 Console, which also includes the Boot Device Management utility. The Console can be installed on any machine that can communicate with the Provisioning Services 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 (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. Re-boot 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 software, then click the **Uninstall** menu option.

Uninstalling the Console

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

Pre-installation tasks

August 29, 2018

You must complete the following tasks before installing and configuring Citrix Provisioning.

> **Important:**
>
> Ensure that all Windows updates are current before installing Citrix Provisioning components. In some cases, you may need to install numerous updates; Citrix recommends that you reboot

> after installing all Windows updates.

Select and configure the Microsoft SQL database

Only one database is associated with a farm. You can can install the Citrix Provisioning database software on:

- An existing SQL database, if that machine can communicate with all Provisioning Servers within the farm.
- A new SQL Express database machine, created using SQL Express, which is free from Microsoft.

In a production environment, best practice is to install the database and Provisioning Server software on separate servers, to avoid poor distribution during load balancing.

The database administrator may prefer to create the Citrix Provisioning database. In this case, provide the MS SQL database administrator with the file that is created using the **DbScript.exe** utility. This utility is installed with the provisioning software.

Database sizing

For information on database sizing, see https://msdn.microsoft.com/en-us/library/ms187445.aspx.

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. This includes the following:

- DatabaseVersion record requires approximately 32 KB
- Farm record requires approximately 8 KB
- DiskCreate record requires approximately 16 KB
- Notifications requires 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 require 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
  - Device:Printer relationship requires approximately 1 KB
  - DevicePersonality requires approximately 1 KB
  - DeviceStatus when a Device boots 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 boots 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: vDisk versioning merge) requires approximately 2 KB
- If auditing is turned on, each change made by the administrator in the 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)**.

If you intend to use the Database Mirroring feature, the SQL native client is required on the server. If

this does not already exist, the option to install SQL native client x64 or x86 is presented when SQL is installed.

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

Database clustering

To implement database clustering, follow Microsoft's instructions then run the Citrix Provisioning Configuration wizard. No additional steps are required because the wizard considers the cluster as a single SQL Server.

Configure authentication

Citrix Provisioning uses Windows authentication for accessing the database. Microsoft SQL Server authentication is not supported except by the Configuration Wizard.

Configuration wizard user permissions

The following MS SQL permissions are required for the user that is running the Configuration wizard:

- dbcreator for creating the database
- securityadmin for creating the SQL logins for the Stream and SOAP services .

If you are using MS SQL Express in a test environment, you can choose to give the user that is running the Configuration wizard sysadmin privileges (the highest database privilege level).

Alternatively, if the database administrator has provided an empty database, the user running the Configuration wizard must be the owner of the database and have the **View any definition** permission (set by the database administrator when the empty database is created).

Service account permissions

The user context for the Stream and SOAP services requires the following database permissions:

- db_datareader
- db_datawriter
- Execute permissions on stored procedures

Datareader and Datawriter database roles are configured automatically for the Stream and SOAP Services user account using the Configuration wizard. The Configuration wizard assigns these permissions provided the user has securityadmin permissions. In addition, the service user must have the following system privileges:

- Run as service
- Registry read access
- Access to Program Files\Citrix\Provisioning Services
- Read and write access to any vDisk location

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.

Because authentication is not common in workgroup environments, 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):

- 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 leverage 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 leverage 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 additional provisioning functionality include:

- Citrix Provisioning XenDesktop Setup wizard, Streamed VM Setup wizard, and ImageUpdate service
  - vCenter, SCVMM, and XenServer minimum permissions
  - Permissions for the current user on an existing XenDesktop controller
  - A Citrix Provisioning Console user account configured as a XenDesktop administrator and added to a PVS SiteAdmin group or higher
  - Active Directory Create Accounts permission to create new accounts in the Console. To use existing accounts, Active Directory accounts have to already exist in a known OU for selection

  - If using Personal vDisks with XenDesktop, the SOAP Server user account must have XenDesktop Full administrator privileges.
- AD account synchronization: Create, Reset, and Delete permissions
- vDisk: Privileges to perform volume maintenance tasks

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

August 30, 2018

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 very common in networks with large groups of users. The use of Citrix Provisioning in the network may 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 this causes 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. To do this, specify all ports to which target devices are connected as edge-ports. This has the same effect as enabling the fast link feature in older switches (disables loop detection).

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

Switch manufacturers

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

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

Using 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. UNC is supported by Windows and many network operating systems (NOSs).

With Citrix Provisioning, UNC format names can be used to specify the location of the OS Streaming database for all Provisioning Servers, and to specify the location of a particular vDisk.

Syntax

UNC names must 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\Provisioning Services
```

> **Note:**
>
> UNC names do not require that a resource be a network share. UNC can also be used to specify a 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 will run. This account must have a password assigned, otherwise the Stream Service will not be able to log in correctly. Your Stream Service can share the same user account and password, or separate user accounts and passwords can be set up for each service.
2. Share the vDisk 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 vDisk 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 on the **Stream Service**, and select Properties.
    - Click the Log On tab. Change the Log on as: setting to This Account, and set up the service to login to the user and password configured in Step 1.
5. Verify that all Stream Services are restarted. The Configuration Wizard does this 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 vDisk 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 do not exist when the services start 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 can also be useful on a diskless system where the disk is actually on the network, using them decreases cache effectiveness and thereby increases network utilization. In an environment that is 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 vDisk

1. Prepare a Standard Image vDisk for configuration.
    - Shut down all target devices that use the Standard Image vDisk.
    - From the Console, change the Disk Access Mode to Private Image.
    - Boot one target device.
2. Configure one or more features.
3. Prepare the Standard Image vDisk for use
    - Shut down the target device previously used to configure the vDisk.

- 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. Consequently, 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 strongly 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. Uncheck 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 the following objects and their associated configuration, administration templates, network or offline files.

- 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 web site and looks for security patches and system updates. If it finds updates that have not been installed, it attempts to download them and install them automatically. Normally, this 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. This is 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.

Re-booting the target device clears both the target device and Citrix Provisioning write cache. Doing this after an auto-update means that the automatic update changes are lost, which defeats the purpose of running automatic updates. (To make Windows updates permanent, you must apply them to a vDisk while it is in Private Image mode, as described below).

To prevent filling your write cache, disable the Windows Automatic Updates service for the target device used to build the vDisk.

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 drop-down list.
10. If the Automatic Updates service is running, click the Stop button 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 vDisk.
2. Change the vDisk mode to Private image.
3. Boot one target device from that vDisk.
4. Apply Windows updates.
5. Shut down the target device.
6. Change vDisk mode to Standard image.
7. Boot all target devices that share this vDisk.

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 the user logs 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 vDisk residing in shared storage. Consequently, the profile returns back to the shared storage containing the vDisk. Since the persistent user data always resides on shared storage, Windows does not need to download the profile. This saves time, network bandwidth, and file cache. Since some of the files included in the profile can grow very 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 vDisk:

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, Logoff
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.

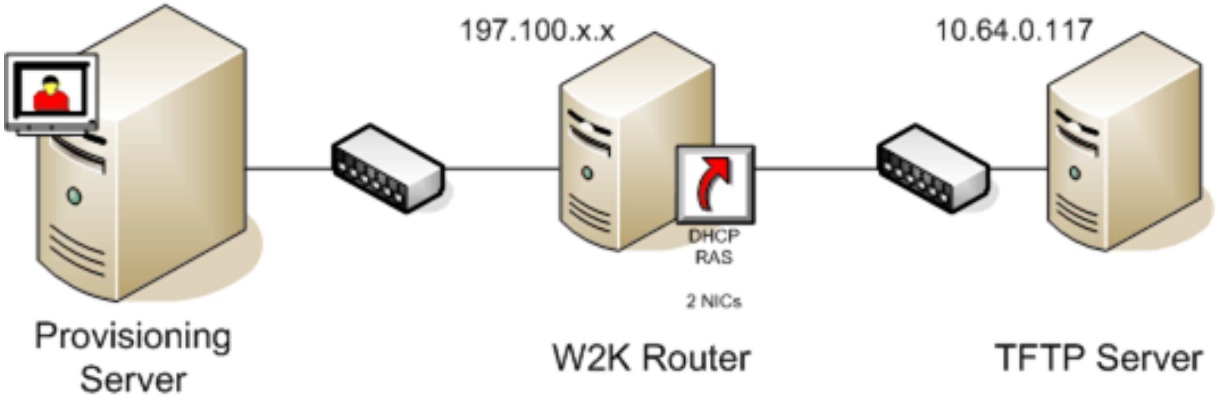
To disable offline folders:

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 user 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 may be needed for different network configurations.

The configuration shown in the diagram below 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, though 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).

In order 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 filename 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 should 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 in the above configuration is not necessary since options 66 & 67 in the router's DHCP service provide the same information to the target device. You can stop the PXE Service on the Provisioning Server if you have no target devices on the Provisioning Server subnet needing its 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. This tag indicates to the target devices (using PXE) 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 provided that the Microsoft DHCP server is installed and configured before installing Citrix Provisioning Services. The Configuration Wizard sets-up the Tellurian DHCP Server configuration file if you use the wizard to configure Provisioning Services.

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

Citrix Provisioning provides the ability to run redundant networks between the servers and the target devices. This requires that both the servers and the target devices be equipped with multiple network interface cards (NICs).

Multiple NICs on the target device may be configured into a virtual team by using Manufacturer's NIC teaming drivers, or into a failover group using the Provisioning Services 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 a host with multiple network

resources, the Citrix Provisioning XenDesktop Setup wizard displays the network resources available to the host and 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 of those devices. Boot devices can include multiple PXE-enabled NICs. Citrix Provisioning uses the first NIC in the list as the primary boot NIC. The primary boot 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 will not be able to locate the target device record in the database (a non-primary NIC may be able to just process the PXE boot phase). Although a workaround would be to add a separate target device entry for each NIC on each system, and then maintain synchronization for all entries, it is not recommended (unless the successful startup of a system is considered as critical as 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 'Moonshot' Mellanox NICS and Intel NIC teaming drivers. A vDisk that is built after configuring NIC teaming can run Standard or Private Image Mode. Broadcom NIC Teaming Drivers v9.52 and 10.24b are not compatible with Citrix Provisioning target device drivers.
- Teaming of multi-port network interfaces is not supported.
- Multi-NIC is supported for XenDesktop Private virtual machine desktops. Using the wizard, Citrix Provisioning allows you to select the network to associate with the Provisioning Services 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.
- Microsoft Windows Server 2012 built-in NIC teaming or OEM NIC teaming software should be installed and configured prior to the Target Device software.
- Configure NIC teaming and verify that the selected teaming mode is expected by the application and the network topology. It should expose at least one virtual team NIC to the operating system.
- When provisioning machines to a SCVMM server, the XenDesktop Setup wizard automatically changes the network configuration of both the first legacy NIC and the second synthetic NIC.
- During the master target device installation process, provisioning target device client drivers need to bind to the new virtual team NIC MAC address. If all physical NICs have been teamed up to a single virtual NIC, the installer automatically chooses the virtual NIC silently, without

prompting.

- If changes are required, Citrix Provisioning Target Device software must be uninstalled before making changes to the teaming configuration, then reinstalled after changes are complete. Changes to teaming configurations on a master target device that has target device software installed, may result 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 works with 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.
- You define the failover group of NICs when you run the Citrix Provisioning target device installer on the Master Target Device. If the machine has more than one NIC, the user is prompted to select the NICs in which to bind. Select all the NICs that participate in NIC failover.
- A target device will only failover 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.
- In the event that 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 essentially instantaneous.
- The NIC failover feature and Citrix Provisioning HA 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 HA rules.
- The next available NIC from the failover group is used should the NIC fail 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 vDisk becomes limited to Private Image Mode. This 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: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\BNIStack\Parameters] DisableHyperVLegacyNic"=dword:00000000
- Load balancing is not supported in the NIC failover implementation.

Update NIC drivers

From time to time, you may need to upgrade the drivers for your network interface cards (NICs). Follow the guidelines below 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 vDisk image.
2. Set the system BIOS to boot from the hard drive.
3. Re-boot the target device directly from the hard drive.
4. Un-install the target device software from this hard drive.
5. Upgrade NIC driver as directed by the manufacturer's instructions.
6. Re-install the target device software on the hard drive.
7. Re-image the hard drive to make a new vDisk image.

> **Note:**
>
> Do not attempt to upgrade a NIC driver on a vDisk. Do not attempt to upgrade a NIC driver on a hard disk on which the Provisioning Server is currently installed. Improperly upgrading a NIC may make 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

August 14, 2018

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

Install any Windows service packs, drivers, and updates before installing the Citrix Provisioning software.

> **Note:**
>
> When installing Citrix Provisioning software on a server that has previous versions of .NET in-

> stalled, Citrix recommends rebooting if prompted to do so during the .NET installation.

1. Click on 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, then enter the folder name or navigate to the appropriate folder where the software should be 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 as well as 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 may take 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 re-run to install additional components at a later time, or re-run 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 that you restart the server after installing the product software, in some instances, a Microsoft message may appear requesting a restart. If this message appears, complete Configuring the Farm using the Configuration Wizard, before restarting the server. If this message appears and the server is not restarted, the removeable drive may not

> appear.

Adding additional Citrix Provisioning Servers

To add additional Citrix Provisioning Servers, install the software on each server that will be 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 new site.

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

Running the configuration wizard silently

August 30, 2018

Silent product software install

Target devices, Citrix Provisioning Servers and Consoles can be silently installed to a default installation directory using the following command:

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

To set a different destination, use the following option:

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

Prerequisite

The Configuration Wizard must first be run on any Citrix Provisioning Server in the farm that has the configuration settings that will be used in order to create the provisioning database and to configure the farm.

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

- Create a ConfigWizard.ans file from a configured Provisioning Server in the farm.

- Copy the ConfigWizard.ans file onto the other servers within the farm, and modify the IP address in the ConfigWizard.ans file to match each server in the farm.
- Run the ConfigWizard.exe with the /a parameter.

To create the ConfigWizard.ans file

1. Run the ConfigWizard.exe with the /s parameter on a configured server.
2. On the Farm Configuration page, choose the Join existing farm option.
3. Continue selecting configuration settings on the remaining wizard pages, then click Finish.
4. Copy the resulting ConfigWizard.ans file from the Citrix Provisioning Application Data directory in \ProgramData\Citrix\Provisioning Services.

To copy and modify the ConfigWizard.ans file

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

To run the ConfigWizard.exe silently

To configure servers, run the ConfigWizard.exe with the /a parameter on each server that needs to be configured.

Note: To get 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 down to the bottom of the file to view all valid parameters.

> **Tip:**
>
> To get a list of commands and their descriptions, use the **/ c** parameter.

Install the Console component

June 21, 2018

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 Provisioning Server software is removed. Upgrading from earlier versions may 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, then enter the folder name or navigate to the folder where the software should be 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 as well as 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 may take several minutes).
11. The 'Installation Wizard Completed' message displays in the dialog when the components and options are successfully installed.

> **Note:**
>
> Re-run the Installation Wizard to install additional components at a later time, or re-run on a different computer to install selected components on a separate computer.

Preparing a master target device for imaging

July 2, 2018

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

> **Important:**
>
> Citrix recommends that you install all Windows updates before installing a PVS target device.

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. This is the hard disk that will be imaged to the vDisk. If necessary, after imaging, the hard disk can be removed from the master target device.

In order to support a single vDisk that is 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 leverage BDM, the master target (prior to vDisk creation) should match the BDM configuration because end target devices use that configuration when booting.

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

If target devices share a vDisk, 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.

Follow the instructions below 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 will be members of a domain, and will share a vDisk, additional configuration steps must be completed.

> **Important:**
>
> Dual boot vDisk images are not supported.

Configuring a master target device's BIOS

The following steps describe how to configure the target device system's BIOS and the BIOS extension provided by the network adapter, to boot from the network. Different systems have different BIOS setup interfaces – if necessary, consult the documentation that came with your system for further information on configuring these options.

1. If the target device BIOS has not yet been configured, re-boot the target device and enter the system's BIOS setup; to get to BIOS 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 may appear differently.

3. Configure the target device to boot from LAN or Network first. Optionally, select the Universal Network Driver Interface; UNDI first, if using a NIC with Managed Boot Agent (MBA) support.

   > **Note:**
   >
   > On some older systems, if the BIOS setup program included an option that permitted you to enable or disable disk-boot sector write protection, ensure that the option is disabled before continuing.

4. Save the changes, then exit the BIOS setup program.
5. Boot the target device from its hard drive over the network to attach the vDisk to the target device.

Configuring Network Adapter BIOS

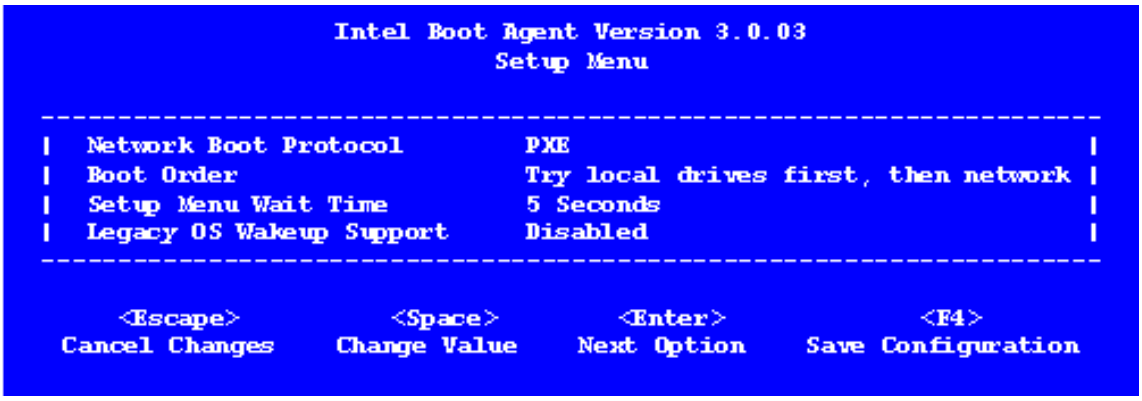
This procedure is only necessary for older systems.

1. Re-boot the Master Target Device.
2. Configure the network adapter's BIOS extension through setup.

   During the system boot, the network adapter's BIOS extension will present an initialization message similar to the following: Initializing Intel ® Boot Agent Version 3.0.03 PXE 2.0 Build 078 (WfM 2.0) RPL v2.43

Enter the network adapter's BIOS extension; consult the network adapter's documentation for more information. The key combination for entering the network adapter's BIOS extension varies by manufacturer. For example, to enter the Intel Boot Agent setup screen, type Ctrl+S.

A screen similar to the following appears:



3. Change the boot order to Network first, then local drives.
4. Save any changes, and exit the setup program. In the Intel Boot Agent, typing F4 saves the changes.

Alternatively, a device can be configured to provide IP and boot information (boot file) to target devices using the Manage Boot Devices utility.

Installing the master target device software

> **Note:**
>
> Before installing the software on a master target device, turn off any BIOS-based-virus protection features. To include anti-virus software on the vDisk image, be sure to turn the anti-virus software back on before running the Imaging Wizard.

Install and configure the Microsoft NIC teaming driver, introduced in Windows Server 2012, or OEM NIC teaming software before installing target device software.

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 vDisk to be mounted to the operating system on the target device.
- **Citrix Provisioning Imaging Wizard**: used to create the vDisk file and image the Master Target Device.

- **Virtual Disk Status Tray Utility**: used to provide general vDisk 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 option you select depends on whether this application will be shared by users on this computer, or whether only the user associated with this computer should have access to 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\Provisioning Services). Optionally, click Change, then either 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 may take several minutes. While the installation process is running, you can clickCancel 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 both .NET 4.5 or newer is installed and Windows Automount is enabled, the Imaging Wizard will start automatically by default (for details, refer to 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 vDisk image.

Using the Imaging Wizard to create a new vDisk

July 2, 2018

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

Prerequisites

Windows NT 6.x:

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

- Each local disk partition is cloned separately to the vDisk. 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.
  - 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

The Imaging Wizard prompts for information that allows for connecting to the farm as well as information necessary to set the appropriate credentials/Active Directory and licensing information to apply to this particular vDisk.

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 name or IP address of a Provisioning Server within the farm to connect to and the port to use to make that connection.
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 select None if volume licensing is not being used:
6. Select to create a new vDisk (default), or use an existing vDisk by entering that vDisk's name, then click Next.
7. If the create new vDisk option was selected, the New vDisk dialog displays:
    a) Enter a name for the vDisk
    b) Select the Store where this vDisk will reside
    c) Select the vDisk format from the appropriate drop-down menus. If the VHDX format is Dynamic, from the VHDX block size drop-down, 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, the MAC address associated with one of the NICs that was selected when the target device software was installed on the master target device, and 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 vDisk is used to boot the VMs) select to optimize the vDisk 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.

Upgrade

October 29, 2018

Citrix Provisioning supports upgrading to the latest product version from versions starting with 7.6 LTSR.

Before attempting to upgrade a Citrix Provisioning farm:

- Select a maintenance window that has the least amount of traffic
- Back up the Provisioning Services database
- Back up all vDisks

> **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 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 contain a minimum subscription advantage (SA) date.
- Back up the Citrix Provisioning database. While Citrix always tests to ensure a successful database upgrade, unforeseen circumstances could arise. Citrix strongly recommends backing up the database before upgrading.
- Back up the Citrix Provisioning vDisk. Citrix recommends backing up the vDisk 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.

> **Note:**
>
> Upgrading Citrix Provisioning requires local administrator privileges.

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 Provisioning Server and Console software at the same time for each Provisioning Server system 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 vDisk 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 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.

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 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

> **Important:**
>
> Citrix strongly recommends backing up the vDisk if versioning is not used in the upgrade process.

When using Citrix Provisioning target installers:

- If the system is running Citrix Provisioning version 7.6.2 (7.6 CU1) or a newer target device, 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.
- If the system is running Citrix Provisioning version 7.6.1 or earlier target devices, uninstall the old target device software. Reboot, then install the new Citrix Provisioning target device version.

In-place upgrades

For in-place upgrades, a maintenance version of the vDisk 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 vDisk.
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 vDisk mode using the maintenance version.
4. Log into Windows and run the new target device installer. Install the software, as if you would 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 into 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 vDisk.

Upgrading using VHD\VHDX boot

When using method to upgrade a target device, consider:

- 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 vDisk 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 vDisk 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. Refer to 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. Refer the following links for creating VMs in Hyper-V. For Hyper-V 2012 R2 and 2016, ensure that the generated VM matches those VMs of the vDisk:

    - Generation 1 = traditional BIOS VMs and systems
    - Generation 2 = UEFI VMs and systems

    For Hyper-V 2016 environments:

    https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/create-a-virtual-machine-in-hyper-v

    For Hyper-V 2012 and 2012 R2:

    https://technet.microsoft.com/en-us/library/hh846766(v=ws.11).aspx

    For Hyper-V 2008 R2 and 2008 R2 Sp1:

    https://technet.microsoft.com/en-us/library/cc956091.aspx

c) Boot the VM.

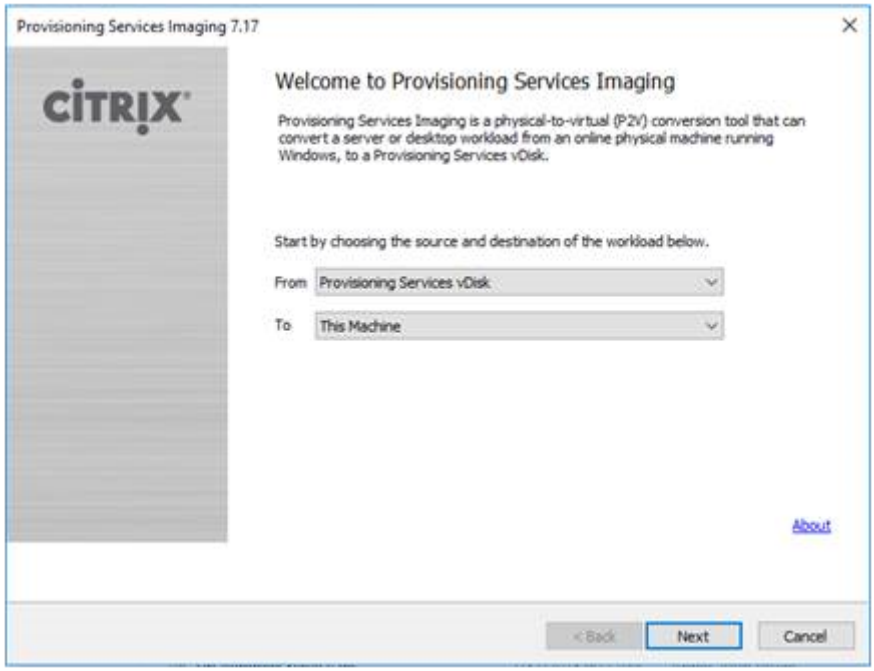
d) Upgrade the target device software. Upgrade the target device software. Refer to the information at the beginning of this section for using the Citrix Provisioning target device installers.

4. Copy the .vhdx.vhd file back to the vDisk 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 vDisk, import the vDisk into the provisioning database using the **Add or import Existing vDisk** option. Run this option from the vDisk 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	Anti-virus updates	Firewall/Network security software
P2PVS reverse imaging	x	x	x	x	x	x	x

Reverse imaging method	Xen tools	VM tools	Hyper-V compati-bility	NIC driver	Windows 10 upgrade	Anti-virus updates	Firewall/Network security software
VHD boot from hy-pervisor	x		x			x	x
Direct VHD boot	x	x	x	x		x	x

1. Boot the Citrix Provisioning target device into the vDisk 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\Provisioning Services Upgrade Wizard.
4. Click the **From** drop-down menu to choose the Citrix Provisioning vDisk. 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 BIOS systems is non-destructive. The partition table of the system is not altered. Because Citrix Provisioning imaging is blocked base, the partition table of the local hard disk must be the same as those of the vDisk.
   > - reverse imaging for UEFI systems is destructive. All partitions on the local hard disk are destroyed and re-created to match those of the vDisk.

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 vDisk again. You can accomplish this imaging by creating a vDisk 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 vDisk.
2. Network boot (PXE/ISO) the VM into the vDisk using maintenance version or private image mode.
3. If the vDisk is using Citrix Provisioning 7.15 or older, install **PVS_UpgradeWizard.exe** or **PVS_UpgradeWizard\x64.exe** from the **Upgrade** folder of the ISO image. This process retrieves the latest **P2PVS.exe** file. The upgrade wizard can also be installed with the Citrix Provisionings meta-installer using the **Target Device Installation > Install Upgrade Wizard** option.
4. Run P2PVS.exe from the Citrix Provisioning target device\ Upgrade Wizard directory. By default, this directory is C:\Program Files\Citrix\Provisioning Services, or C:\Program Files\Citrix\Provisioning Services Upgrade Wizard, respectively.
5. Click the **From** drop-down menu and choose **Citrix Provisioning vDisk** and click **Next**.
6. 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**.
7. Click **Convert** on the last page to begin reverse imaging.
8. Once reverse imaging has completed successfully, set the VM to boot from HDD and reboot the VM.
9. Uninstall the Citrix Provisioning target device.
10. 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.

11. 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 C:\ partition.

12. Boot the VM. Please note the local admin of the VM and remember the local admin password.
13. Run Windows 10 update to upgrade Windows 10.
14. You may have to use local admin credentials to log in since the Windows 10 upgrade process can impact active directory.

15. Rejoin the VM to active directory if needed.
16. Install new drivers and more Windows updates if needed.
17. Once updates are done, install Citrix Provisioning target device software.
18. Use the Imaging Wizard or P2PVS to create a vDisk. The old vDisk can be used if the size of the VM's virtual hard disk has not been increased in step 11.

Servers

September 26, 2018

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 the farm. While the first Provisioning Server is being upgraded, some administrative features are not available. Citrix recommends closing all Consoles until the upgrade is complete to avoid failed operations. When upgrading a server, the Console component is also upgraded.

> **Note:**
>
> The Upgrade Wizard must be installed and run in a folder that does not contain surrogate pair characters (Unicode code point after 0x10000).

Upgrading the first Provisioning Server

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 Console on this server or on a server used to manage the farm. For details on installing the Console, refer to 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, refer to the instructions on how to join an existing farm in Configuration Wizard Tasks.

Upgrading remaining Provisioning Servers in the farm

Complete the same procedure that was performed on the first server on each of the remaining servers in the farm.

> **Tip:**
>
> The database upgrade is ignored because the database was upgraded 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 Provisioning Server.

To perform the rolling server upgrade, update the first Provisioning Server in the farm:

1. Open the services MSC file (services.msc) 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:

   a. 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.

   b. 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, 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. At this point, if the provisioning database has not been upgraded, a message appears indicating that the database is upgraded. Click **OK**.

   Verify that all Citrix Provisioning services have started as intended using **services.msc** and boot a target device to confirm connectivity to the Provisioning Server.

   After upgrading the first Provisioning Server in the farm, upgrade all other servers:

3. Open the services MMC file (services.msc) 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.
4. The configuration wizard automatically starts after clicking Finish once the Provisioning Server has been successfully upgraded.

   > **Note:**
   >
   > The provisioning database is updated by the first Provisioning Server.

5. 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.
6. Repeat steps 3–5 to upgrade all other Provisioning Servers in the farm after upgrading the first server.

vDisks

August 30, 2018

> **Important:**
>
> Backup all vDisks before upgrading to a newer product version.

Upgrading vDisks involves installing the new version of the Provisioning Services target device software on the vDisk image.

If you are upgrading from Citrix Provisioning 7.6.1 or later, you can do an in-place upgrade. Citrix recommends that you use this method if possible. 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.

If you have to upgrade from versions earlier than 7.6.1, the following vDisk upgrade methods are supported:

- Upgrading vDisks using Hyper-V. If you are upgrading from Citrix Provisioning 6.x to 7.1 or 7.6, this inline upgrade method is recommended because it is faster than re-imaging, and uses the least amount of storage.
- Upgrading vDisks by re-imaging. If neither of the other two methods of upgrading vDisks are viable in your implementation, select from one of the following re-imaging upgrade methods:

- **Versioned vDisk Upgrade:** If upgrading vDisks from Citrix Provisioning 6.x to 7.1 or 7.6, use this vDisk upgrade method if the Upgrading vDisks using Hyper-V method cannot be used. This method re-images to a maintenance version of the vDisk, allowing production devices to continue running and booting from the production version of the vDisk. After the upgraded version of the vDisk is promoted to production, target devices will boot or reboot from the upgraded vDisk version.
- **Automated Inline Upgrade:** If upgrading vDisks from Citrix Provisioning 5.1.x, 5.6.x, or 6.x to 7.1 or 7.6, use this method if the Upgrading vDisks using Hyper-V or Versioned vDisk Upgrade methods cannot be used. This method uses the Upgrade Wizard and Upgrade Manager to automate some of the steps included in the Manual vDisk Upgrade method.
- **Manual vDisk Upgrade:** If upgrading from 5.1.x, 5.6.x, or 6.x to 7.1 or 7.6, using this vDisk upgrade is recommended only if the Upgrading vDisks using Hyper-V or Versioned vDisk Upgrade methods cannot be used, or the Automated Inline Upgrade method fails. It may also be considered if multiple partitions exist on the vDisk and the same system and machine are available for re-imaging (the hard disk drive does not need to be the same).

Upgrade a vDisk using Hyper-V

If you are upgrading from Citrix Provisioning 6.x to 7.1 or 7.6, this inline upgrade method is recommended because it is faster than re-imaging, and uses the least amount of storage.

Before upgrading using Microsoft Hyper-V, review the following requirements:

- General Hyper-V knowledge.
- Hyper-V must be installed (Hyper-V does not need to be installed on the Provisioning Server).

> **Note:**
>
> Hyper-V upgrade does not support vDisks using 16 MB block size. When creating new vDisk images, the block size should be 2 MB or greater.

1. On a Hyper-V server, uninstall previously installed Provisioning Services software.
2. Install the newer version of Citrix Provisioning software.
3. Copy a newly created VHDX file to the Hyper-V server:
    a) Create a new version of the vDisk.
    b) Promote the new version to test mode.
    c) Perform a merge base to test mode.
    d) Copy the VHDX from step c to the Hyper-V server
4. Create a new virtual machine in the Hyper-V Manager.
5. During the creation steps, attach the existing newvDisk.vhdx instead of using a new VHDX.
6. Go into the properties of the newly created Hyper-V virtual machine (Action panel > Settings) and remove the Network adapter. Go to Add Hardware and add the Legacy NIC.

7. Go to the Legacy NIC and attach it to the physical system's NIC.
8. Boot the virtual machine.
9. Let the system install the new drivers, then reboot if prompted.
10. Uninstall Citrix Provisioning target device software, then reboot.
11. Optional: Install Hyper-V's Integration Services. This is only necessary when the resulting VHDX must be bootable in both physical and virtual systems. While the virtual machine is on, go to Action, then choose Insert Integration Services set up disk, then install.
12. Install Citrix Provisioning target device software.
13. Choose to bind Citix Provisioning to the inactive NIC (the physical NIC from the original target device). When installing 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.
14. Shut down the virtual machine.
15. Go to the virtual machine's properties (Action panel > Settings), then set it to boot to the legacy NIC first.
16. Transfer the VHDX (newvDisk.vhdx) back to the Provisioning Server.
17. From the Citrix Provisioning Console:
    a) Add the VHDX to the Citrix Provisioning database using the Add existing vDisk menu option.
    b) Add the Hyper-V virtual machine to the list of the target devices.
    c) Associate the vDisk with the appropriate target devices.
    d) Set the vDisk to Standard Image Mode
18. Boot the physical target device (assuming this is set to PXE first), then the Hyper-V virtual machine.

The original vDisk is now upgraded and a common image for the physical and virtual machines has also been created.

Upgrade a vDisk using Reverse Imaging

Upgrade by re-imaging only if neither of the other two methods of upgrading vDisks (in-place upgrade from version 7.6.1 and later, or upgrading using Hyper-V) is viable in your implementation.

The re-imaging upgrade method that you choose will depend on your existing Citrix Provisioning implementation and network requirements.

Versioned vDisk upgrade

This vDisk upgrade method can be selected when upgrading vDisks from 6.x to the latest version of the target device software. This method re-images to a maintenance version of the vDisk, allowing production devices to continue running and booting from the production version of the vDisk. After

the upgraded version of the vDisk is promoted to production, target devices will boot or reboot from the upgraded vDisk version.

Upgrade prerequisites include:

- Upgrading all Provisioning Servers
- Upgrading Provisioning Consoles
- Creating a backup copy of the vDisk

To upgrade, complete the following procedure:

1. Boot the Maintenance device from the managed vDisk while in **Maintenance mode**.
2. From the product installation directory, run P2PVS.exe to reverse image using volume-to-volume imaging. Select the vDisk 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 new vDisk image, create the target device if it does not already exist, and assign the vDisk to the target device.
6. Test streaming the new vDisk image by booting a Maintenance or Test device from the upgraded vDisk.

Manual reverse imaging using P2PVS

When manually performing reverse imaging using P2PVS, consider the following:

- Boot the provisoning target device into the vDisk using private\maintenance mode.
- Install PVS_UpgradeWizard.exe or PVS_UpgradeWizard_x64.exe from the Upgrade folder of the ISO image of the latest Citrix Provisioning release 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\Provisioning Services UpgradeWizard).
- Click the **From** drop down menu and choose **Provisioning Services vDisk** and click **Next**.
- In the partition screen, select the partitions that will be reverse imaged. All system partitions, regardless of whether they have a drive letter or not, will be used in reverse imaging. Click **Next**.
- Click **Convert** on the last page to begin reverse imaging.

> **Note:**
>
> Reverse imaging for BIOS systems is non-destructive. The partition table of the system will not

> be altered. Because PVS imaging is blocked base, the partition table of the local hard disk must be the same as those of the vDisk.
> **Important:**
>
> Reverse imaging for UEFI systems is destructive. All partitions on the local hard disk will be destroyed and re-created to match those of the vDisk.

About reverse imaging on UEFI VMs

Reverse imaging can be used to update antivirus and malware definitions, however, UEFI cannot perform this task as BIOS can perform it.

When reverse imaging UEFI VMs, consider the following:

- Reverse imaging UEFI VMs can only be done manually using P2PVS.exe, using either:
  - GUI
  - Command line

> **Important:**
>
> When using reverse imaging on UEFI VMs, consider that the process is destructive, all data will be lost as a result.

Automated inline upgrade

Use the Automated vDisk Upgrade method when upgrading from 5.1.x, 5.6.x, or 6.0 to 6.1, and the Hyper-V upgrade method cannot be used. This upgrade method takes an existing vDisk and converts it to the current product version using the Upgrade Wizard and Upgrade Manager.

Prerequisites:

- All Provisioning Consoles have been upgraded.
- All Provisioning Servers have been upgraded.
- A copy of the vDisk has been created prior to upgrading.

Automated Inline vDisk upgrades require that the vDisk is offline to target devices until the vDisk upgrade completes. To avoid vDisks being offline, create a clone of the vDisk and use it for the upgrade process. Then, after the upgrade completes, target devices can be migrated to the upgraded vDisk.

1. On the master target device or maintenance device, depending on the target device platform, run either PVS_UpgradeWizard.exe or PVS_UpgradeWizard_x64.exe.
2. Copy UpgradeManager61.exe from the Provisioning Services 6.1 Target Device product installation directory into the installation directory of the Provisioning Server. The default product installation directory is C:\Program Files\Citrix\Provisioning Services.
3. On the Provisioning Server, run UpgradeManager61.exe.

4. On the master target device, run UpgradeConfig.exe from the Windows Start menu shortcut or from the product installation directory:
    a) Specify a local account with Administrator privilege to AutoLogon. This local account cannot have an empty password.
    b) Specify a local partiton to which reverse imaging will clone data. The original hard drive that the vDisk was cloned from is recommended.
    Note: If this is a new hard drive, use the manual upgrade method to initialize the hard drive.
    c) Specify the Provisioning Server IP address and a user account and password to connect to UpgradeManager. This account cannot have an empty password.
    d) Click OK.
    e) UpgradeConfig preforms a sanity check on various parameters. If everything passes, the UpgradeConfig exits, and then reboots the machine to start the upgrade script.
    f) The machine will reboot several times, and then display a message to indicate that the script has successfully completed.

> **Note:**
>
> **AutoLogon** clears when the upgrade completes. If you are using AutoLogon for vDisk deployment, setup AutoLogon as necessary.

Upgrading vDisks manually

Use the manual upgrade as a universal approach to upgrading vDisks, or if any of the following are true:

- The vDisk has gone through a number of 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 vDisk 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 vDisk file.
4. Boot from the vDisk.

Image back to master target device's hard drive

There are two procedures that allow you to image a vDisk 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 vDisk was created; this 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 vDisk was created

1. Boot from the vDisk 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 located at \Program Files\Citrix\Provisioning Services\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 should point to the vDisk first partition by default.
7. Proceed cloning the hard drive image to the vDisk Destination Drive.
8. To connect the vDisk 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 will not be able to connect with the vDisk.
9. Uninstall the product software. For details, refer to the section about removing PVS.

Image back using an unformatted, uninitialized hard disk drive

1. Boot from the vDisk 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 vDisk.
7. Run the Image Builder utility on the target device. This utility is located at \Program Files\Citrix\Provisioning Services\P2PVS.exe.
8. Specify the destination drive letter of the newly created partition (or the original boot HDD partition) as the vDisk. The vDisk should first point to the destination drive partition by default.
9. Clone the hard drive image to the vDisk Destination Drive.
10. To connect the vDisk 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 will not be able to connect with the vDisk.
11. Uninstall the product software. For details, refer to thesection about removing Citrix Provisioning.

Install master target device software

Complete the following steps to install the latest product software on the Master Target Device.

1. Run the new 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 vDisk file:

1. Run the Image Builder utility on the target device. This utility is located at \Program Files\Citrix\Provisioning Services\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 should point to the vDisk first partition by default.
3. Clone the hard drive image to the vDisk Destination Drive.

Boot from the vDisk

Using the Console, set the target device on the Provisioning Server to boot from vDisk, then reboot the target device. The new target device should now be running the new vDisk image.

Upgrade a target vDisk using in-place upgrade

Use the information contained in this article to upgrade a PVS target device vDisk 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 Citrix Provisioning 7.6.1 and newer, the target being upgraded must have been installed using the PVS target install method, and not upgraded using binary replacement.

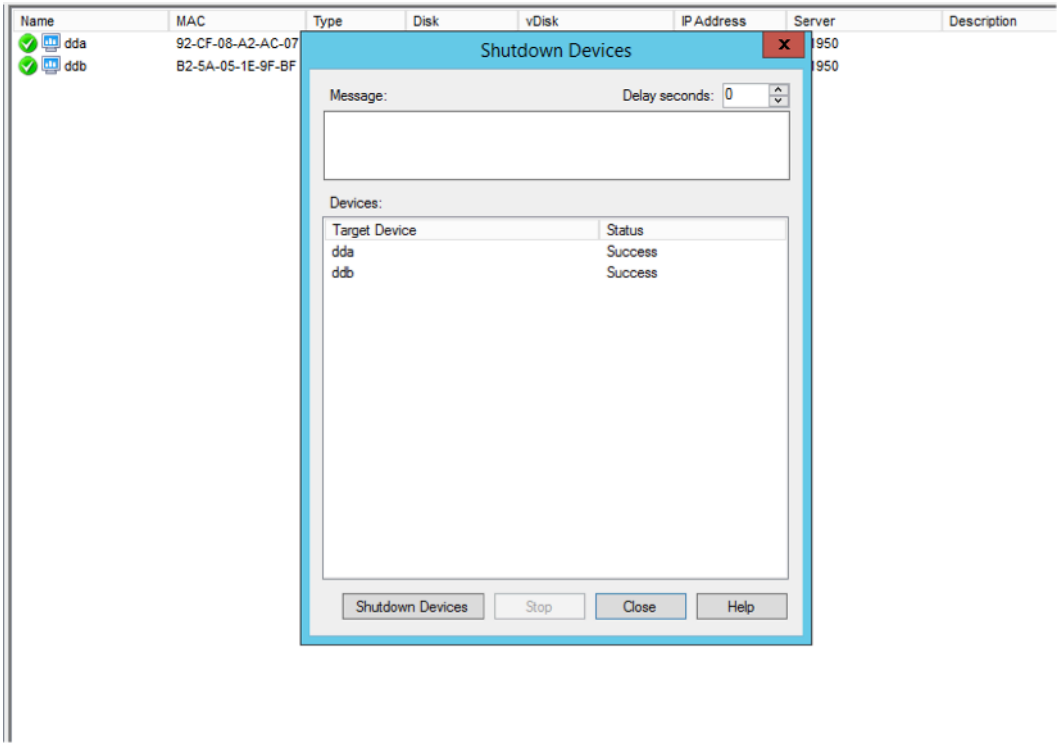
Boot a target device into private image mode or a maintenance version

Use the information in this section to boot a target device in either private image mode, or to boot in maintenance mode.

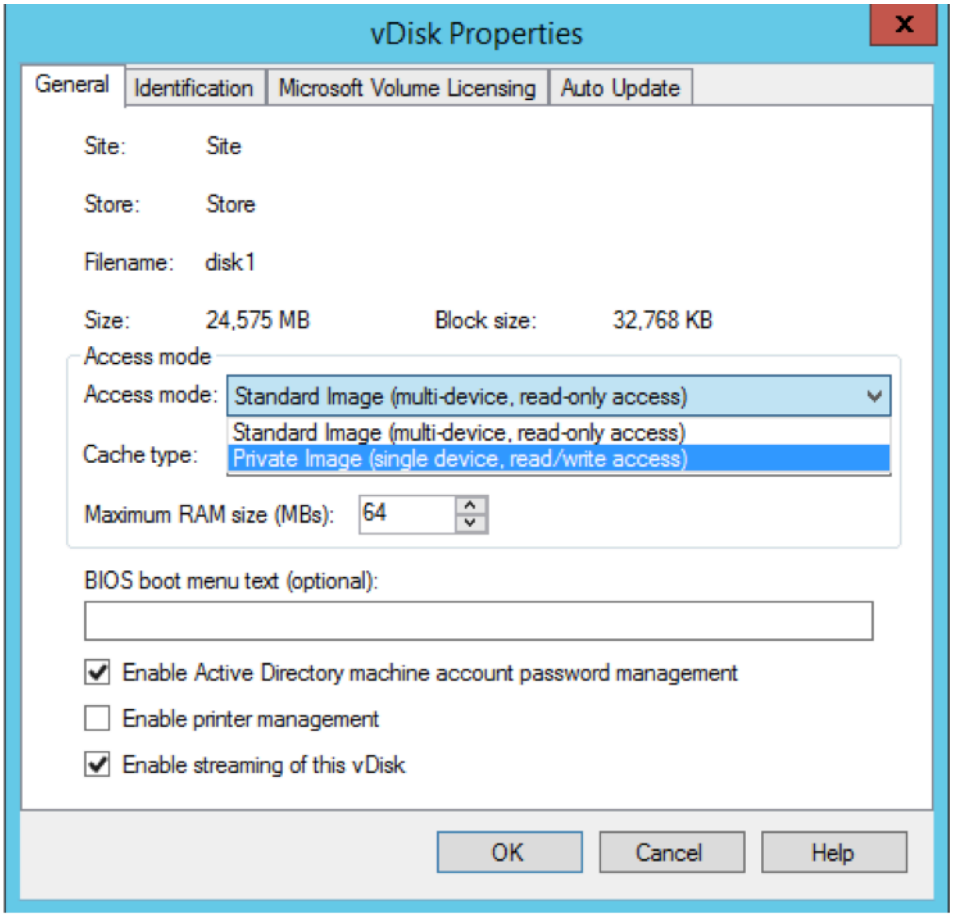
> **Tip:**
>
> Before booting from private image mode, Citrix recommends that you backup the vDisk before attempting an upgrade.

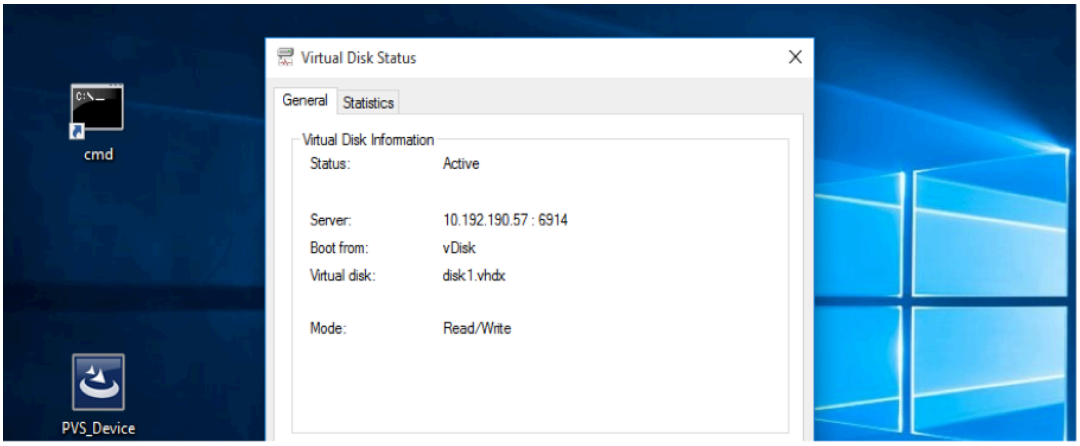
Boot in private image mode

1. Shutdown all other devices.



2. Set the vDisk that you want to upgrade to **private image mode**:
    a) Open the vDisk's properties dialog by right clicking the vDisk, and choose **Properties**.
    b) From the **Access** mode group, select **Private Image** (single device, read/write access):



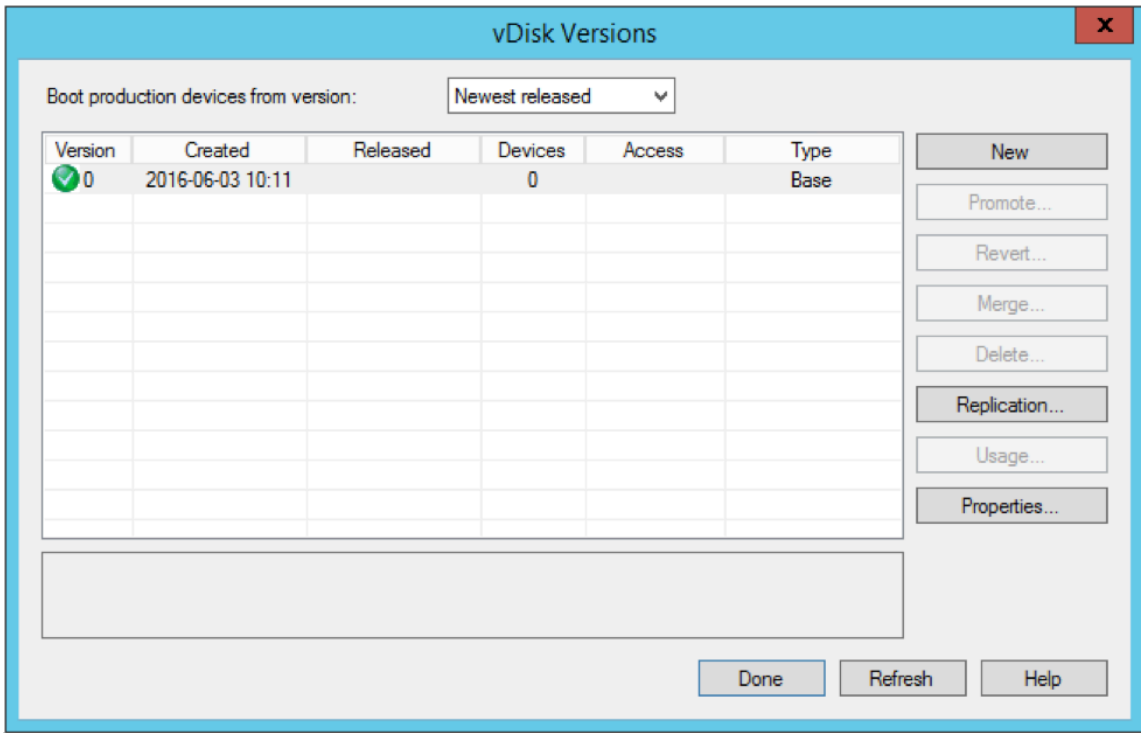


3. Boot a target device using that vDisk:

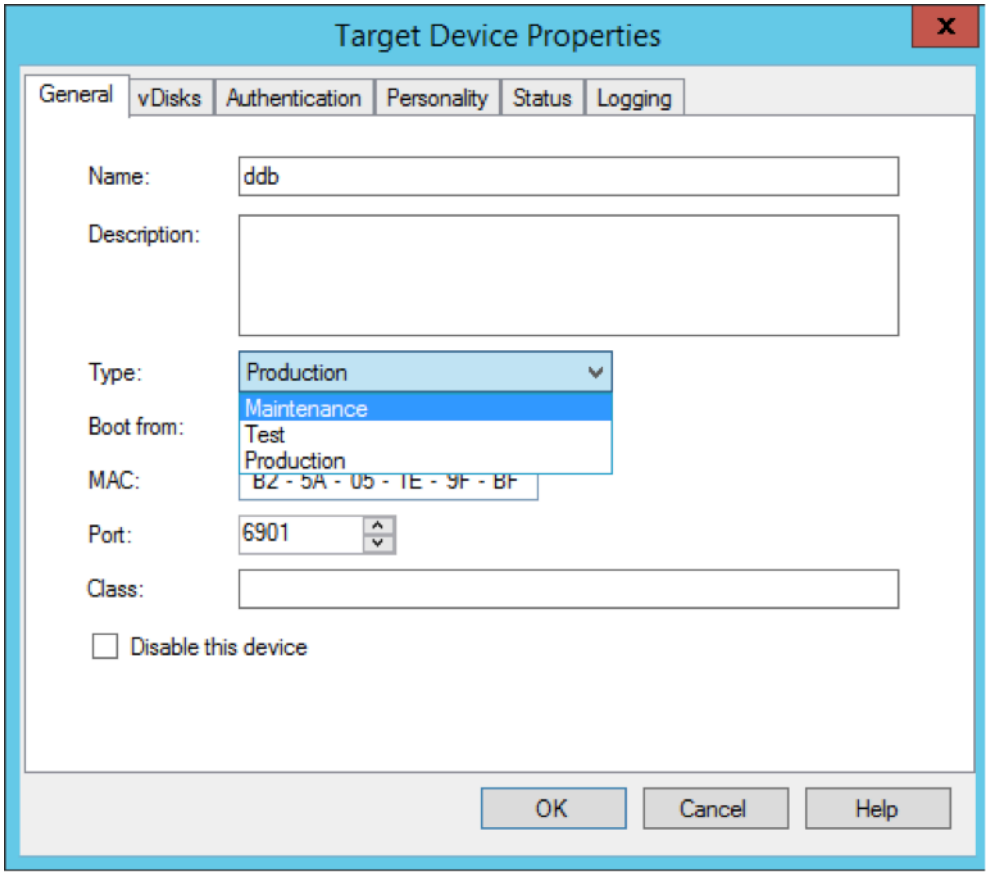
Boot in maintenance mode

1. Right click the standard mode vDisk and choose the option **Versions...** to open the vDisk Versions screen.
2. Click the **New** button (in the upper right portion of the interface) to create a maintenance vDisk

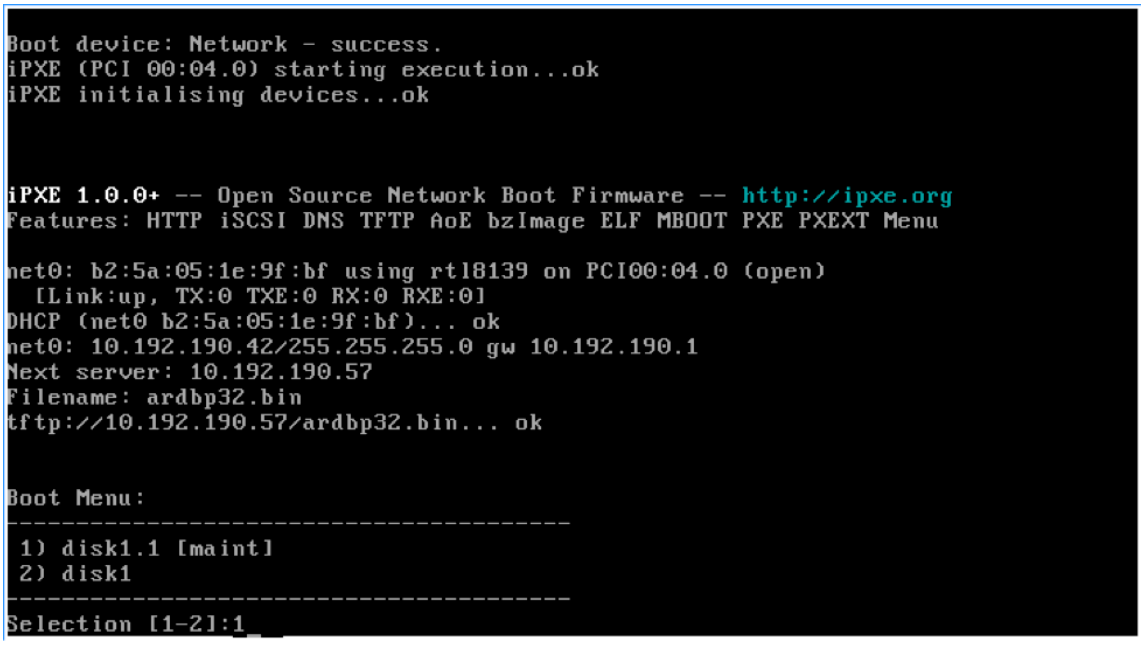
version:



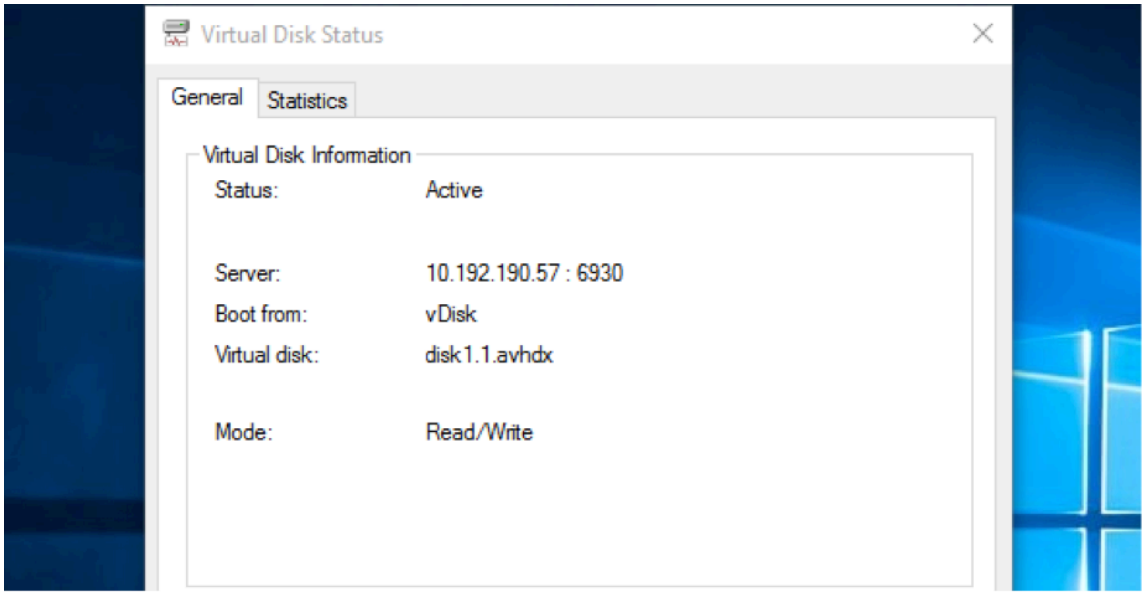
3. Set a target device that is using that vDisk to maintenance mode by right clicking on the target, then choose the **Properties** option.
4. Choose **Maintenance** from the drop-down menu for the property type:



5. Boot a target device using the specified vDisk version.
6. Choose **option 1** from the boot menu that appears when booting the target device:



7. The provisioning status tray of the device should resemble:



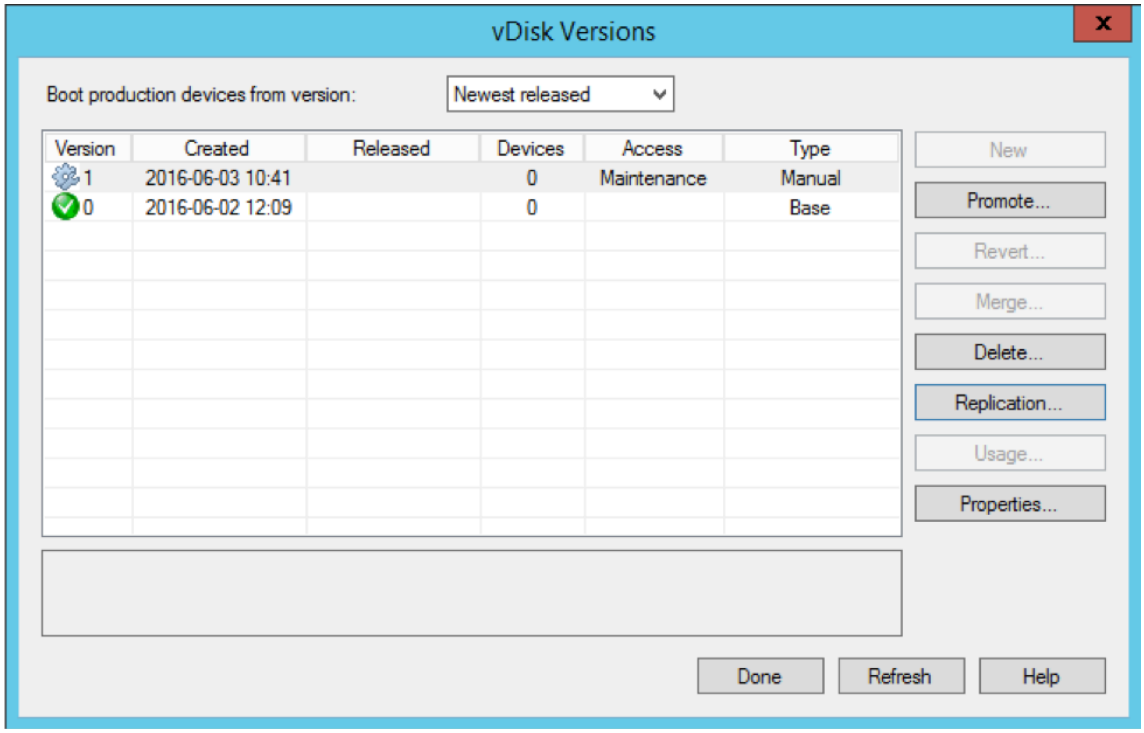
> **Tip:**
>
> The virtual disk's name should be followed by a **.x** where **x** is greater than or equal to 1 and the extension should be **.avhdx** or **.avhd**.

Upgrade 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 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. Shutdown the target device.
7. Open the vDisk version interface (refer to step 1 above).
8. Click **Promote** to promote the vDisk to either a test or production version:



> **Tip**
>
> The **New** button should be greyed out and inaccessible.

a) **Test version** - This should be used to verify the vDisk is fully operational before promoting it to the production version.

b) **Production version** - This represents the version used by all users in a full roll out of the vDisk to the production environment.

Configure

August 9, 2018

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 (referrred to as the vDisk) in read-only format to the target device which resides in a collection. These target devices communicate with the Provisioning Server. For more information, refer to the Citrix Provisioning architecture article.

Console

August 30, 2018

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 Console

Before starting the Console, make sure that the Stream Service is started and running on the 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, then select the New Window from Here menu option.
- A new Console window opens. It may be necessary to 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 should be saved.
3. Type or select the file name in the File name textbox.
4. Select the file type from and Save as text boxes. 1. 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 checkbox next to each MMC and Snap-in view option that should display 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(s) to select object-related tasks. For a complete list of tasks, refer to that object's management chapter within this guide.
- **Drag and drop:** Using the Drag-and-Drop 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 vDisk to all target devices within a collection by dragging the vDisk and dropping it on the collection. The vDisk and the collection must be in the same site; the new vDisk assignment replaces any previous vDisk 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 vDisks assignments that were specific to this server and any store information will be 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 vDisk, 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:
  1. 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.
  2. Place a check in the checkbox next to each of the object properties you want to copy, then click OK.
  3. In the Console tree, expand the directory where the object exists so that those objects display in either the tree or details pane, 4) Right-click on the object(s) 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 drop-down menu, select the device collection where the target devices to add are 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, refer to Managing Views.

Configuring the bootstrap from the Console

For the Provisioning Server to start a target device, a boot file is downloaded by the Citrix Provisioning MBA or PXE-compliant boot ROM, when the device is turned on. 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, refer to 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.

Field	Description
IP settings	The IP Address, Subnet Mask, Gateway, and Port for up to four Provisioning Servers, which will perform login processing.
Add	Click the Add button to add a new Provisioning Server to the file. Up to four Provisioning Servers may be specified for 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 Provisioning Servers. The order in which the Provisioning Servers appear in the list determines the order in which the Provisioning Servers are accessed should a server fail.
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 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 a primary and secondary DNS and Domain be identified.

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 and the Use DHCP to retrieve Device IP option is selected (under Device IP Configuration settings), your DHCP server needs to provide option 6 (DNS Server).

  > **Note:**
  >
  > If using HA, 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 Provisioning Server information, then click OK to exit the dialog: IP Address, Subnet Mask, Gateway, Port (default is 6910).

  > **Note:**
  >
  > If using high availability (HA), enter up to four Provisioning Servers. If you are not using HA, only enter one. Use the Move Up and Move Down buttons to sort the Provisioning Servers boot order. The first Provisioning Server listed will be 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 work with newer Windows OS versions and is enabled by default. Only disable this setting if your target device is hanging or behaving erratically in early boot phase.

Field	Description
Network recovery method	This field includes: **Restore Network Connections**; Selecting this option results in the target device attempting indefinitely to restore it's 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 will fail and the system will reboot to the local hard drive. The default number of seconds is 50, to be compatible with HA 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 server that responds is used. In non-HA systems, 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 will switch from one server to the next in trying to find an active one. The valid range is from 1,000 to 60,000 milliseconds.

Field	Description
Login general timeout	Enter the time-out, in milliseconds, for all login associated packets, except the initial login polling time-out. This time-out is generally longer than the polling time-out, because the Provisioning Server needs time to contact all associated servers, some of which may be down and will require retries and time-outs from the server to the other servers to determine if they are online or not. The valid range is from 1,000 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 Provisioning Server setup. Because the server returns the list of bootstrap files found under Citrix Provisioning Program Data, 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 can not be configured from the Console and target devices will fail to boot; receiving a 'Missing TFTP' error message.

   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 should only be 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:
    - Select the Verbose Mode option if you want to monitor the boot process on the target device (optional). This enables system messaging on the target device.
    - Select Interrupt Safe Mode if the target device hangs early in the boot process.
    - Select Advanced Memory Support option to enable the bootstrap to work with newer Windows OS versions (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 it's connection to the Provisioning Server.
    - Reboot to Hard Drive - 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 can not be established, PXE will fail and the system will reboot 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 that this could result in sub-optimal performance. It is recommended that NTFS be used 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 server that responds 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 will switch from one server to the next, in trying to find an active server. The valid range is from 1,000 to 60,000 milliseconds.

    Login General Timeout

Enter the time-out, in milliseconds, for all login associated packets, except the initial login polling time-out. The valid range is from 1,000 to 60,000 milliseconds.

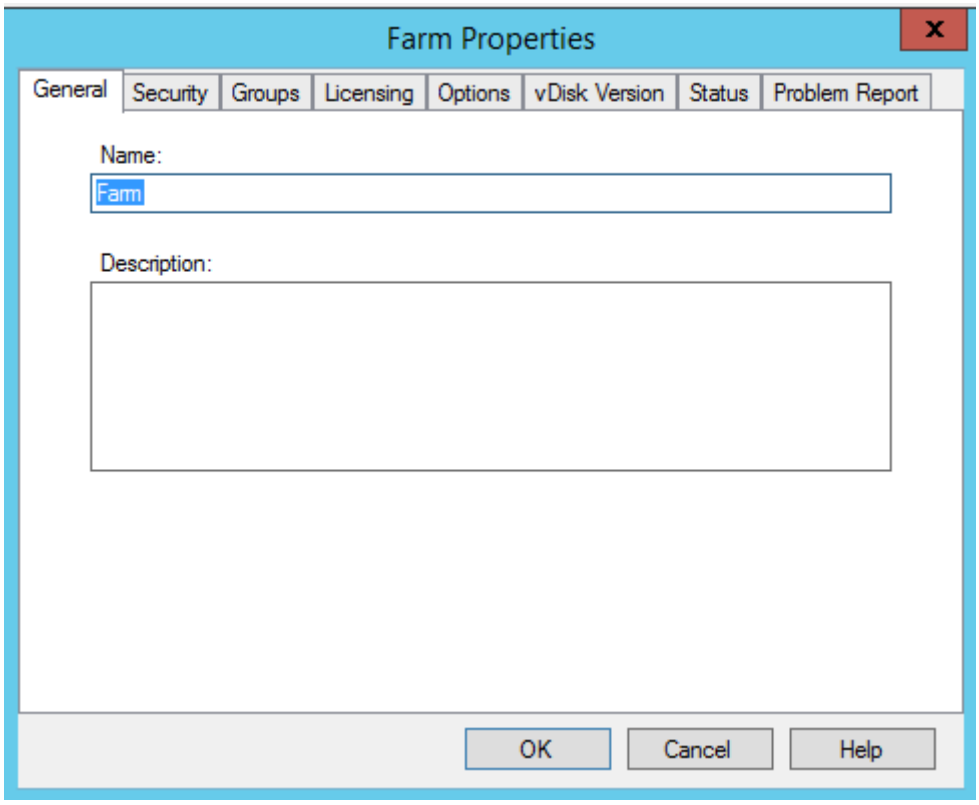
6. Click OK to save your changes.

Farm

September 13, 2018

Use the information in this section to configure a farm using the Provisioning Console. This section includes information about the following elements:

- General Tab
- Security Tab
- Groups Tab
- Licensing Tab
- Options Tab
- vDisk Version Tab
- Status Tab
- Problem Report 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 button	Click the **Add** button to apply farm administrator privileges to a group. Check each box next the groups to which farm administrator privileges should apply.
Remove button	Click the **Remove** button to remove groups from those groups with farm administrator privileges. Check each box next the groups to which farm administrator privileges should not apply.

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 select 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 checkboxes next to each group that should be included in this farm. **Note:** Filtering on groups was introduced in 5.0 SP2 for efficiency purposes.

Field	Description
Remove button	Click the **Remove** button to remove existing groups from this farm. Highlight the groups to which privileges should not apply.

Licensing tab

Field	Description
License server name	Type the name of the Citrix License Server in this textbox.
License server port	Type the port number that the license server should use or accept the default, which is 27000.

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 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:** This feature should only be enabled when expecting to add new target devices. Leaving this feature enabled could result in computers being added without the approval of a farm administrator.
Auditing	Enable or disable the auditing feature for this farm.
Offline database support	Enable or disable the offline database support option. This option allows Provisioning Servers within this farm, to use a snapshot of the database in case the connection to the database is lost.

vDisk version tab

Field	Description
Alert if number of versions from base image exceeds:	Set an alert should the number of versions from the base image be exceeded.
Default access mode for new merge versions	Select the access mode for the vDisk 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 vDisk update, if over alert threshold	Enable automatic merge. Check to enable the automatic merge feature should the number or vDisk versions exceed the alert threshold. Minimum value is 3 and Maximum value is 100.

Status tab

Field	Description
Status of the farm	Provides database status information and information on group access rights being used.

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.

Configuration Wizard settings

Before running the Configuration Wizard, be prepared to make the following selections (described in detail below):

- Network Topology
- Identify the Farm
- Identify the Database
- Identify the Site
- License Server Settings
- Select **Network Cards** for the Stream Service
- Configure Bootstrap Server

> **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. Refer to the installation article for information about the Linux streaming component.

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**.

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 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
     - Provisioning Services 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
     Select this option to reconfigure an existing farm, then continue on to the "Configure user account settings" procedure. This option only appears if a farm exists.
   - Create farm
     a) On the **Farm Configuration** dialog, select the **Create Farm radio** button to create a farm, then click **Next**.
     b) Use the **Browse** button to browse for existing SQL databases and instances in the network, or type the database server name and instance. Optionally, enter a **TCP port number** to use to communicate with this database server.
     Note: The combination of the database name and farm name should not exceed 54 characters. In such cases, the farm name may display as a truncated entry in the **Existing Farms** screen.
     c) To enable database mirroring, enable the Specify database mirror failover partner option, then type or use the **Browse** button to identify the failover database server and instance names. Optionally, enter a **TCP port number** to use to communicate with this server.
     d) Click **Next** to continue to the next step, select the database location.
   - Join existing farm
     a) On the **Farm Configuration** dialog, select the **Join Existing Farm** radio button to add this Provisioning Server to an existing farm, then click **Next**.
     b) Use the **Browse** button to browse for the appropriate SQL database and instance within the network.

c) 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.
d) To enable database mirroring, enable the Specify database mirror failover partner option, then type or use the **Browse** button to identify the failover database server and instance names. Optionally, enter a **TCP port number** to use to communicate with this server.
e) Click **Next**.
f) Select from the following site options, then click **Next**:
   - Existing Site: Select the site from the drop-down menu to join an existing site.
   - New Site: Create a site by typing the name of the new site and a collection.

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 may be a staged database.
      Note: When rerunning the Configuration Wizard to add extra Provisioning Servers database entries, the Server Name and Instance Name text boxes are already populated. By default, SQL Server Express installs as an instance named 'SQLEXPRESS'.
   c) 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 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 the restored database on the **Existing Farm** dialog.
   g) Select the site that the Server was previously a member of on the **Site** dialog.
   h) 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 drop-down list, 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 may 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 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 may prompt the user to join a store or create a store, but 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. You can do this 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

Select the license server

1. Enter the name (or IP address) and port number of the license server (default is 27000). The Provisioning Server must be able to communicate with the license server to get the appropriate product licenses.
2. Optionally, select the check box **Validate license server version and communication**. This option verifies that the license server is able to communicate with this server and that the appropriate version of the license server is being 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.

3. Click **Next** to continue on to configure user account settings.

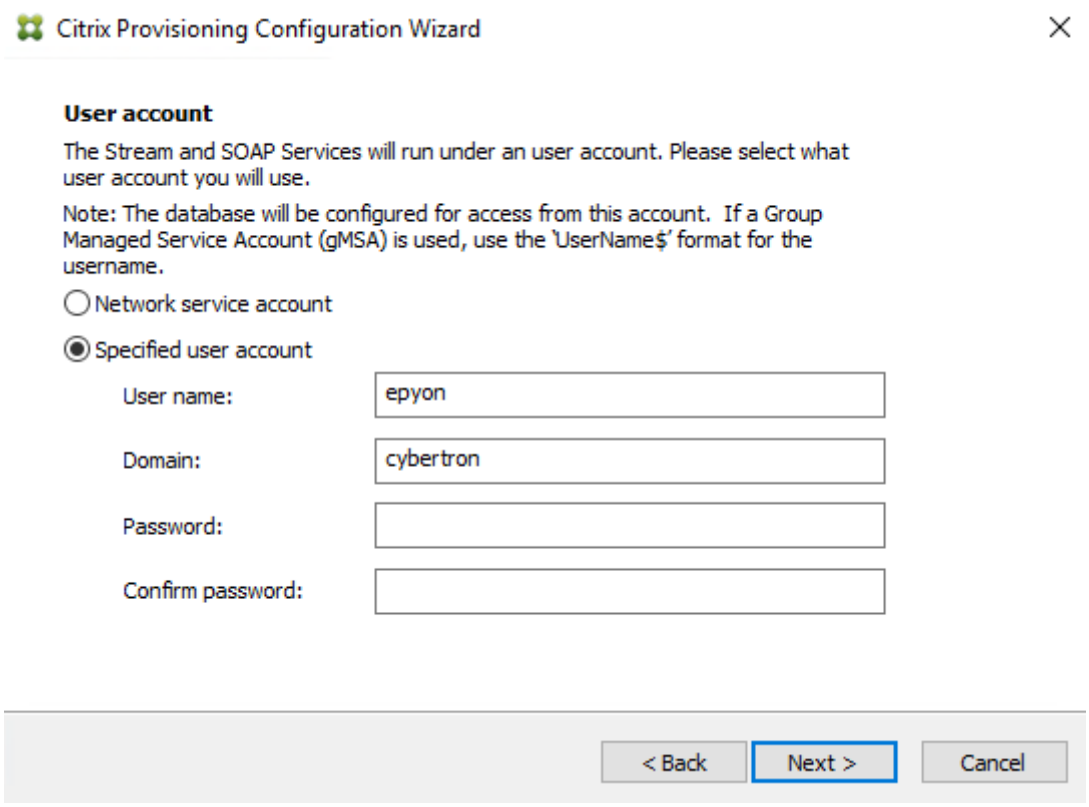
Configure user account settings

The Stream and Soap services run under a user account. To provide database access privileges to this user account, Data reader and Data writer database roles are configured automatically using the Configuration wizard.

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.



Creating self-signed certificates for Linux streaming

When configuring Citrix Provisioning for streaming Linux Desktops, the Linux target devices must be linked to the Provisioning Soap server via an SSL connection. The CA certificate must be present on both the Provisioning Server and the target device.

Using the Citrix Provisioning Configuration Wizard, you can choose to add the proper certificate from the provisioning Soap container, specifically for Linux Desktops.

Creating self signed certificates with PoSH

To create a certificate:

1. Use the following PowerShell command (as an administrator) to create a self-signed certificate that is placed into the provisioning Soap container:

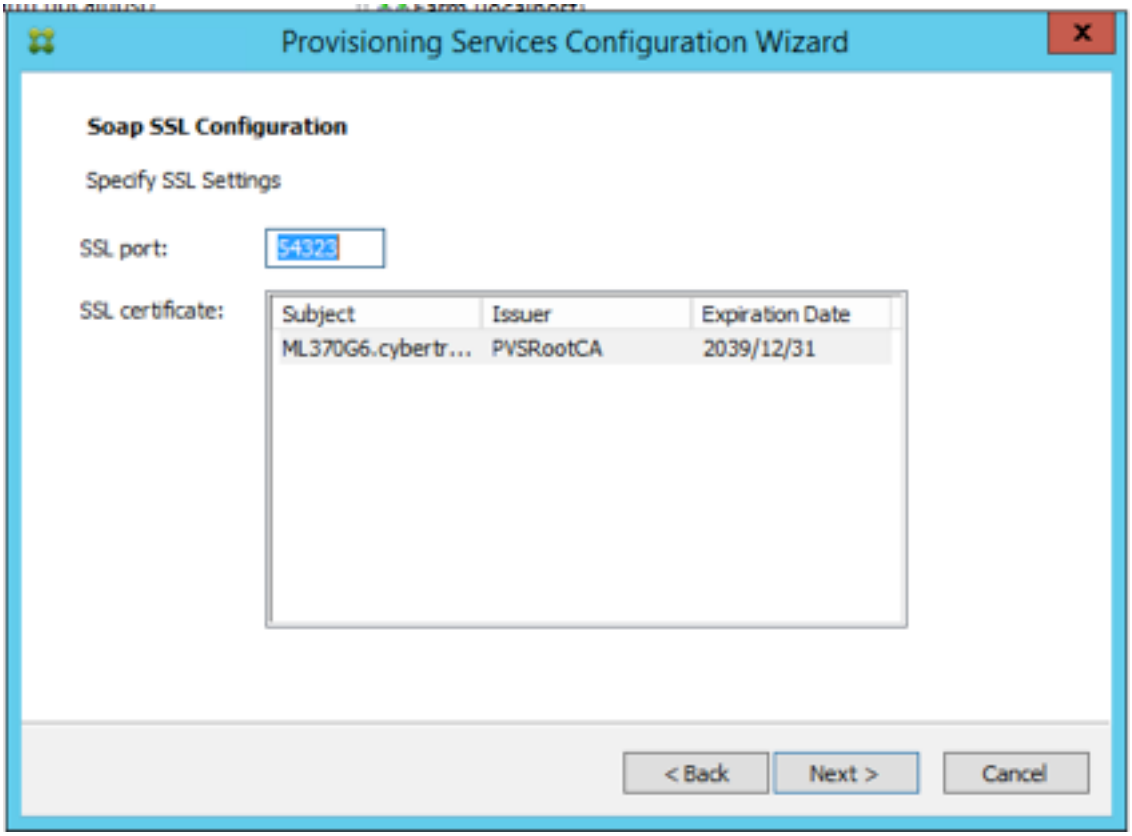
```
#New-SelfSignedCertificate -Type SSLServerAuthentication -Container
    PVSSoap -Subject "CN=PVS-01.fqdn" -CertStoreLocation "Cert:\
    LocalMachine\My" -KeyExportPolicy Exportable
```



```
PS C:\Windows\system32> New-SelfSignedCertificate -Type SSLServerAuthentication -Container PVSSoap -Subject "CN=PVS-01.shilllabs.local"

   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject
----------                                -------
DE36C7895BA9C5E94C73A71545FB02587326092F  CN=PVS-01.shilllabs.local
```

2. Import the generated certificate into the local machine's Trusted Root Certificate Authority store from the Personal store.

3. Run the Citrix Provisioning Configuration Wizard. At the Soap SSL Configuration prompt, choose the newly generated certificate by highlighting in blue, and continue through the wizard:



> **Tip:**
>
> When the **Soap SSL Configuration** page first loads the certificate is highlighted (in gray) which gives the appearance that it is selected. **Ensure that the certificate is selected**. It should turn blue to indicate that it has been selected.

Select network cards for the Stream Service

1. Select the check box next to each of the network cards that the Stream Service can use.
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

1. Select the bootstrap server. To use the TFTP service on this Provisioning Server:
   a) Select the Use the TFTP Service option, then enter or browse for the boot file. The default location is: C:\Documents and Settings\All Users\ProgramData\Citrix\Provisioning Services\Tftpboot
   If a previous version of Citrix Provisioning was installed on this server, and the default location is:
   C:\Program Files\Citrix\Provisioning Services\TftpBoot
   run the Configuration Wizard to change the default location to:
   C:\Documents and Settings\All Users\ProgramData or ApplicationData\Citrix\Provisioning Services\Tftpboot
   If the default is not changed, the bootstrap file cannot be configured from the Console and target devices fail to boot. The message 'Missing TFTP' appears.
   b) Click **Next**.
2. 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 Remove to remove the Provisioning Server from the list. Use the Move up or Move down buttons to change the Provisioning Server boot preference order. The maximum length for the server name is 15 characters. Do not enter the **FQDN** for the server name. In an HA 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 will 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 work with newer Windows OS versions and is enabled by default. Disable this setting on Windows Server OS 32 bit versions that do not support PAE. 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 will reboot to the local hard drive. The default number of seconds is 50, to be compatible with HA configurations.
- **Logon polling timeout:** Enter the time in milliseconds between retries when polling for Provisioning Servers. Each Provisioning Server is sent a login request packet in sequence. The first server that responds 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 Provisioning Server to the next in trying to find an active server. The valid range is from 1,000 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. This time-out is longer than the polling time-out. This is because the Provisioning Server needs time to contact all associated servers, some of which may be down. 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 to 60,000 milliseconds.

3. Verify that all configuration settings are correct, then click **Finish**.

Bootstrap configurations can be reconfigured by selecting the Configure Bootstrap option from the **Provisioning Services Action** menu in the Console.

Server

October 25, 2018

You typically perform the following tasks when configuring Provisioning Servers in your farm.

> **Important:**
>
> After making any changes to 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 Provisioning Server, changes could prevent the device from reconnecting. The IP address field on the Network tab must reflect the real static IP address of the Provisioning Server.

Provisioning Server properties

On the Console, the Provisioning Server Properties dialog allows you to modify Provisioning Server configuration settings. 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 if a change made on a Provisioning Server Properties dialog requires that the server be rebooted.

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.

Field	Description
Power rating	A power rating is assigned to each server, which is then used when determining which server is least busy. The scale to use is defined by the administrator. For example, an administrator may decide to rate all servers on a scale of 1 to 10, or on a scale of 100 to 1000. Using the scale of 1 to 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 target devices. Likewise, when using a scale of 100 to 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.

Server tab

The following options are assessible 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 is consumes more system resources.

Field	Description
Buffers per thread	Number of packet buffers allocated for every thread in a thread pool. The number of buffers per thread should be large enough to enable a single thread to read one IO transaction from a target device. So buffers per threads should 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 considered 'Up' 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 will attempt to write its status information every (Server cache timeout/2) seconds, i.e. 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.

Field	Description
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 the Citrix Provisioning service is a highly multi-threaded service, it is possible for it to send hundreds of simultaneous I/O requests to a given storage device. These are usually queued up 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. By throttling the concurrent I/O transactions in the Citrix Provisioning Service, better performance can be achieved with these types of devices. 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. This a simple way to achieve separate limits for network shares and for local drives. If you have a slow machine providing a network share, or slow drives on the machine, then a count of 1 to 3 for the remote limit may be necessary to achieve 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 might be desirable on very fast local drives. If a network share is overloaded, you'll see a lot more device retries and reconnections during boot storms. This is caused by read/write and open file times > 60 seconds. Throttling the concurrent I/O transactions on the share reduces these types of problems considerably.

Field	Description

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 may be needed to prevent IP fragmentation. Citrix Provisioning does not currently support IP fragmentation and reassembly. Also, if you are using a device or software layer that adds bytes to every packet (for security reasons for example), a smaller value may be needed. If your entire infrastructure supports jumbo packets (Citrix Provisioning NIC, target device NIC and any intervening switches and/or routers) then 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 that will be transmitted in a single read/write transaction before an ACK is sent from the server or device. The larger the IO burst, the faster the throughput to an individual device, but the more stress placed on the server and network infrastructure. Also, larger IO Bursts increase the likelihood of lost packets and costly retries. Smaller IO bursts reduce single client network throughput, but also reduce server load. Smaller IO bursts also reduce the likelihood of retries. IO Burst Size / MTU size must be <= 32, i.e. only 32 packets can be in a single IO burst before a 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 will be told to pause if the Maximum devices booting limit has been reached. The device will display a message to the user and then wait Boot pause seconds before attempting to continue to boot. The device will continue 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 will be considered in the booting state. Once a device starts to boot, the device will be considered booting until the Maximum boot time has elapsed for that device. After this period, it will no longer be considered booting (as far as boot pacing is concerned) even if the device has not actually finished booting. Maximum boot time can be thought of as a time limit per device for the booting state for boot pacing.
Maximum devices booting	The maximum number of devices a server allows to boot at one time before pausing new booting devices. The number of booting devices must drop below this limit before the server will allow more devices to boot.
vDisk creation pacing	Amount of pacing delay to introduce when creating a vDisk on this Provisioning Server. Larger values increase the vDisk 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 this long.

Network tab

Field	Description
IP address	The IP addresses that the Stream Service should use for a target device to communicate with this Provisioning Server. When adding a new Provisioning Server, enter the valid IP address for the new server. The following fields are including when viewing IP address information: **Add** — Add an IP address for the selected Provisioning Server; **Edit** — Opens the IP address dialog so that the IP address for the selected Provisioning 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.

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 so that a new store and that store's properties can be included in the list of stores, which overrides 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.

Field	Description
Store properties	Includes the following fields: **Store** — The name of the store. This field displays when editing an existing store. If this is a new store, select the store from the drop-down list; **Path** used to 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 setting an override store path on the Server's Properties dialog, the path must be set prior to creating a new version of the vDisk. Because this path information is stored and referenced in the .vhdx header information, changing the path after versioning may cause 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, and use the slider to set the number of days between renegotiation.
Enable automatic vDisk 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 could not recover from.
File size maximum	Enter the maximum size that a log file can reach before a new file is created.

Field	Description
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 checkbox next to each property to copy, or click the Select all button to enable all properties to be copied.
3. Click Copy. Right-click on the Provisioning Server that you want to copy properties to, then select Paste.

Configuring Provisioning Servers manually

If you are setting up a remote Provisioning Server, or have special requirements, you will need to configure and start your Stream Services manually. The Configuration Wizard needs to be run on remote Provisioning Servers to insure that all settings are configured properly. Failure to run the Configuration Wizard may make it impossible for you to map a vDisk.

Re-running the Configuration Wizard

The Configuration Wizard can be used when updating the Stream Service if the IP address of your Provisioning Server changes. If you change your Provisioning Server's IP address for any reason, simply re-run the Configuration Wizard and choose the new IP address when prompted to do so. 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. It is highly recommended to set the service to start automatically each time a Provisioning Server boots.

> **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.

The Stream Service needs to be started in order 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, it may be necessary to delete a Provisioning Server from the list of available Provisioning Servers in a farm.

> **Note:**
>
> Before you can delete a Provisioning Server, you must first mark the server as down or take the server off line, otherwise the Delete menu option will not appear. The Stream Service can not be deleted.

When you delete a Provisioning Server, you do not affect vDisk image files or the contents of the server drives. However, you do lose all paths to the vDisk image files on that server.

After deleting a Provisioning Server, target devices are no longer assigned to any vDisk image files on that server. The target device records remain stored in the Virtual LAN Drive database, but the device cannot access any vDisk 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 vDisk directory prior to deleting.

To delete a Provisioning Server:

1. In the 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 Provisioning 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.

Starting, stopping or restarting a server

> **Tip:**
>
> Starting, stopping, or restarting Citrix Provisioning may result in unexpected behavior. For more information, see Servers.

To start, stop, or restart Provisioning Services on a Provisioning Server:

1. Highlight the Provisioning Server in the Console, than select the Stream Services menu option from the Actions menu, right-click menu, or Actions pane. The Provisioning Server Control dialog appears.
2. Select from the following menu options:
3. Highlight the Provisioning Servers that you want to take action on, 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, install the **subinacl** tool from Microsoft https://www.microsoft.com/downloads/details.aspx?FamilyID=e8ba3e56-d8fe-4a91-93cf-ed6985e3927b&displaylang=en, then use the following command line to set the permissions on the StreamService:

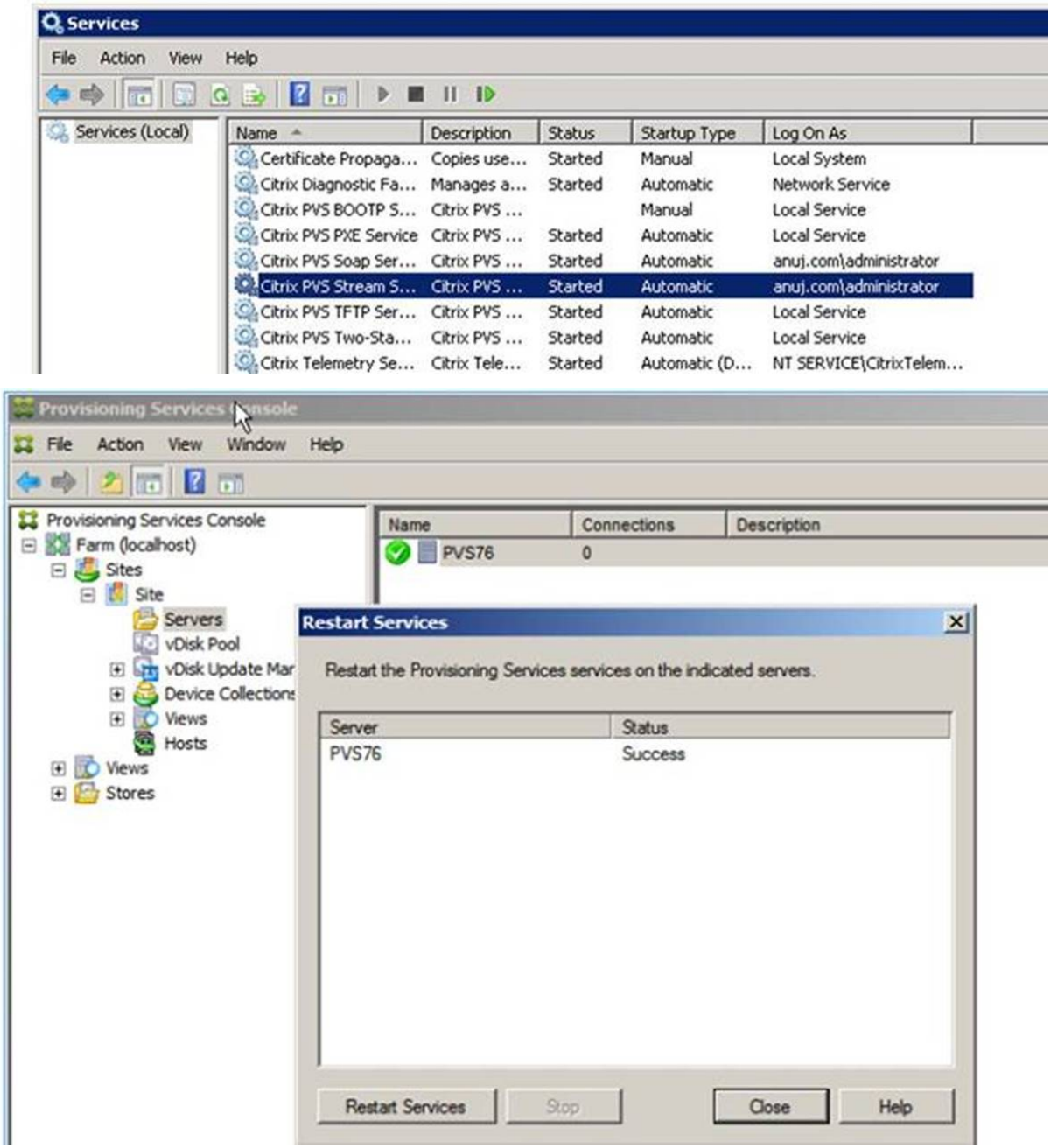
```
subinacl /service streamservice /grant=NetworkService=TOP
```

Citrix Provisioning Console fails to restart or stop

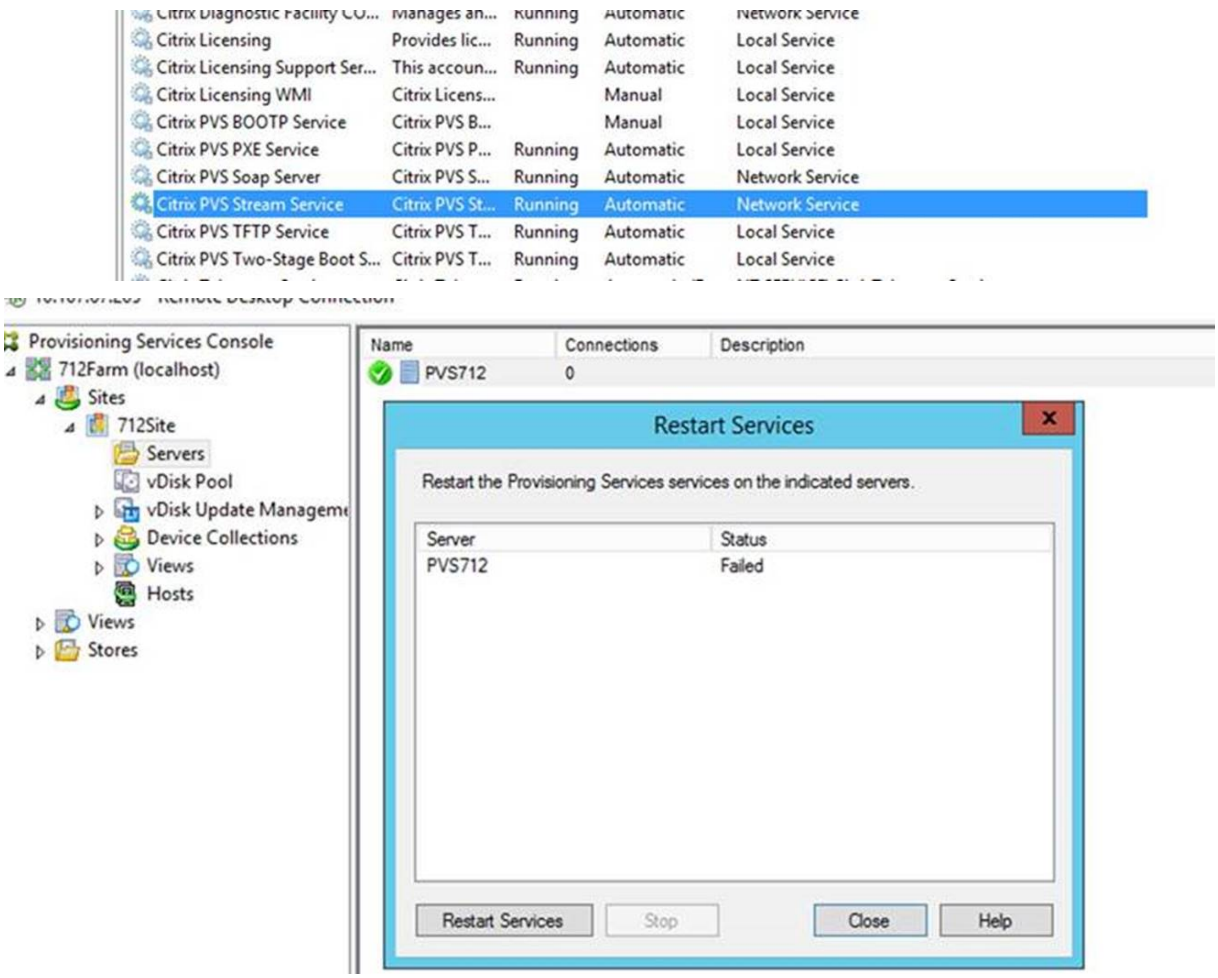
In some cases, the Console may fail to restart or stop services when running a stream service with a network service account. When this occurs, the service appears in the started state, however, the console prevents you from restarting or stopping the stream service.

> **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 vDisk, however, the service cannot be restarted or stopped:



You may be able to resolve this issue by associating the stream service with a specific account which has the required permissions to access the database. For example, if the services are configured with a specifc account (e.g., `anuj.com\administrator`), the status appears as started, and you can restart or stop the services from the Provisioning Console:



Device collections

August 29, 2018

Device collection properties are located on the following tabs:

- General
- Security
- Auto-Add

General tab

Field	Description
Name	The name of this device collection.
Description	Describes this device collection.

Field	Description
Template target device	To use the settings of an existing target device as the template to apply to all target devices that are added to this collection, select that device from the drop-down menu, then click **OK**.

Security tab

Field	Description
Groups with Device Administrator access	Assign or unassign device administrators to this collection using Add or Remove. Device administrators can perform tasks on all device collections to which they have privileges.
Groups with Device Operator access	Assign or unassign device operators to this collection using Add or Remove. Device operators have the following privileges:Boot and reboot a target device, Shut down a target device, View target device properties, View vDisk properties for assigned target devices

Auto-Add tab

Field	Description
Template target device	Displays the name of the target device, if a device was previously selected, or <No template device>, if a device was not selected. Use the drop-down menu to select a device to use as the template for adding new devices to this collection. To view a selected device's properties, click **Properties** (read-only dialog appears).

Field	Description
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 in combination 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’ and stops naming or adding devices after the number reaches ‘999’.Enable the Zero fill option to automatically add the necessary number of preceeding zeros to a numbers length. For example, if the numbers length is equal to 3,than the first target device number would be assigned as ‘001’. Enable the Zero fill option to automatically add the necessary number of preceeding zeros to a numbers length. For example, if the numbers length is set to ‘4’, than 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 in combination 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 new device collection:

1. In the Console, right-click on the Device Collections folder where the new collection will exist, 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, and 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 deletes any target device member records within the collection. The records can be recreated 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 dragged and dropped to other collections, then the original collection can be deleted. If a device collection needs to be moved to a different site or that site becomes obsolete, you can use the export and import features to add the devices to a collection in another site, then the original collection can be deleted.

To delete a device collection:

1. In the 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

August 21, 2018

After installing and configuring Citrix Provisioning components, a vDisk is created from a device's hard drive by taking a snapshot of the OS and application image, and then storing that image as a vDisk file on the network. The device that is used during this process is referred to as a master target device. The devices that use those vDisks are called target devices.

Configuring target devices that use personal vDisks

Citrix XenDesktop with personal vDisk technology is a high-performance enterprise desktop virtualization solution that makes VDI accessible to workers who require personalized desktops using pooled-static virtual machines.

Target devices that use personal vDisks are created using the Citrix XenDesktop Setup Wizard. Within a Citrix Provisioning farm, the wizard creates and adds target devices with personal vDisks to an existing site's collection and assigns an existing shared-mode vDisk to that device.

The wizard also creates virtual machines to associate with each device. A type of catalog in Citrix Desktop Studio that allows you to preserve the assignment of users to desktops (static assignment); the same users are assigned the same desktop for later sessions. In addition, the wizard creates a dedicated storage disk (before logon) for each user so they can store all personalization's to their desktop.

Personalizations include any changes to the vDisk image or desktop that are not made as a result of an image update, such as application settings, adds, deletes, modifications, documents.

Target devices that use personal vDisks can only inherit properties from another device that uses personal vDisks.

> **Tip:**
>
> Use the Device with Personal vDisk Properties dialog on the Provisioning Services console to configure, view, or modify the properties of a target device that uses a personal vDisk.

General tab

To update read-only fields, the device needs to be deleted and re-created with the XenDesktop Setup Wizard.

Menu option	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. This field is read-only. If the target device is a domain member, it should use the same name as in the Windows domain, unless that name is the same as the machine name being imaged. When the target device boots from the vDisk, the name displayed here becomes the target device machine name.
Description	Provides a description to associate with this target device.
MAC	The media access control (MAC) address of the network interface card that is installed in the target device. This field is read-only.
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 the same port), you must change this value.

Menu option	Description
vDisk	Name of the vDisk that this device uses. This field is read-only.
Change	Use to change the vDisk assignment for this device. The Assign vDisk dialog displays with the currently assigned vDisk's Store information. The vDisk you select must be from the same vDisk base image as the previous image.
Personal vDisk drive	Drive letter from which the personal vDisk is accessed. Default is P: (range allowed is between E: to U: and W: to Z:). This field is read-only.

Personality tab

Menu option	Description
Name and string	There is 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 "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

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 that the version is in Production (it cannot be in Maintenance or Test).
- License information; depending on the device vendor, displays product licensing information (including; n/a, Desktop License, Datacenter License, XenApp License, or XenDesktop License).

Logging tab

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 could not recover from.
- Error— Logs 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.

Personal vDisk test mode

Use the personal vDisks test device to test vdisk updates for a device that uses personal vDisks within a test environment. Using the PvD production environment, you can then test for compatibilty with your actual environment.

Considerations

- Personal vDisk devices can be test or production devices.
- Citrix Provisioning displays an appropriate error message when trying to boot a private image or a maintenance version with a personal vDisk device. Only devices without personal vDisks disk can boot a private image or maintenance version.
- You can change the vDisk assignment in the Citrix Provisioning console with these methods:

  - Change assignment with Target Device properties vDisk tab.
  - Copy and paste target device properties.
  - Drag and drop a vDisk to a collection or a view.
- Informational warning displays when changing vDisk assignment for personal vDisk devices.
- Changing personal vDisk device type requires additional privileges for the soap/stream services user.
  - Local administrator on the Citrix Provisioning server system.
  - XenDesktop full administrator.
  - Full permission to the XenDesktop database (this is a XenDesktop requirement).
- For merging, Citrix Provisioning automatically reboots devices and personal vDisk runs inventory when needed.
- Citrix recommends that you dedicate a small group of personal vDisk devices for test mode in their own catalog. Also, keep this desktop group in maintenance mode when not used; otherwise, XenDesktop power management is in control and turns devices on and off. This may potentially interfere with merging.
- By default, Studio does not show the personal vDisk stage. You should add that column.
- The personal vDisks test mode environment requires that two catalogs are available: one for personal vDisk test devices and the other for personal vDisk production devices. If you want to use this feature in an environment where both personal vDisk test and production devices exist in one catalog, changing a production personal vDisk device to test causes all devices in that catalog to reboot. Change the production personal vDisks devices to test devices before creating any test version vDisk.

SCCM interoperability

When using SCCM and a provisioned device:

- Add the command *C:\Program Files\Citrix\personal vDisk\Bin\CtxPvd.exe* to the shutdown script
- Updates typically require numerous reboots, as a result, you must inventory all provisioned devices each time you reboot or shutdown a device.

About PVD test devices

Use the information in this section when using PVD devices in a provisioned environment:

- PVD devices should either be in *test* or *production* mode.
- Citrix Provisioning displays an error message when you try to boot a private or maintenance version with a PVD device. Only devices without a PVD disk can boot a private image or maintenance version.
- A vDisk assignment can be changed in the Citrix Provisioning Console using the following methods:

  - Changing the assignment using the device's properties.
  - Copying and pasting the device's properties.
  - Dragging and dropping the vDisk to a collection or a view.
- Citrix Provisioning displays an informational warning when you change the vDisk assignment for a PVD device.
- Changing the PVD device type requires more privileges for the SOAP/Stream Service user:
  - Local administrator privileges on the Provisioning Server system.
  - Full administrator privileges on the Citrix Virtual Apps and Desktops system, including the database
- When merging, Citrix Provisioning automatically reboots devices. A PVD device runs an inventory, as needed.
- Citrix recommends that you allocate a small group of PVD devices for *test mode*. This group of PVD devices should be kept in *maintenance mode* when not in use. Otherwise the Citrix Virtual Apps and Desktops power management feature initializes these devices, potentially interfering with the merge process.

Consider:

- this environment is suitable when two catalogs are available, one for PVD test and another for PVD production devices. If you want to use this feature in an environment where both PVD test and production devices exist in the same catalog, change a production PVD device to *test*. This process causes all devices in that catalog to reboot.
- changing production PVD devices to *test* **before** creating any test versions of a vDisk.

Assign or reassign a vDisk to a target device that uses a personal vDisk

You can assign a different vDisk to a target device that uses a personal vDisk if that vDisk is from the same base (.vhdx) vDisk lineage. For example, to update an existing vDisk you can make a copy of the target device's currently assigned vDisk, update the new vDisk, then assign the updated vDisk to the device.

To assign or reassign a vDisk:

1. On the Device with Personal vDisk Properties dialog's General tab, click Change…. By default, the Assign vDisk dialog displays with the current vDisks Store location and lists all vDisks available from that Store, with the exception of the currently assigned vDisk.
2. In the Filter section, you have the option to:

   a. Change the Store location from which to select vDisks from.

   b. Filter vDisks that display in the list based on the server's that can deliver them.
3. Select the vDisk to assign to this target device.

Adding target devices to the database

To create new target device entries in the Provisioning Services 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. Refer to 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, refer to "Enabling Automatic Password Management".

3. Optionally, if a collection template exists for this collection, you have the option to enable the checkbox 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.

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, refer to Importing Target Devices into Collections.

Using the Auto-Add Wizard

The Auto-Add Wizard automates the configuration of rules for automatically adding new target devices to the Provisioning Services 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 that the Auto-Add Wizard was started from.

A Farm Admininistrator has the ability to turn Auto-Add on or off and to select the default Site.

A Site Admininistrator only has the ability to select the default site if the current default site is a site in which that administrator is the Site Administrator. If the Site Administrator is not the Administrator of the currently selected default Site, then that administrator can only configure the sites they has access to.

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 drop-down list, select the site where devices should be 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 drop-down list, then click Next. The Select Template Devices page appears.
6. Select the device to use as a template, so that new devices being added will 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 in combination 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', Provisioning Services starts naming 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 preceeding zeros to a numbers length. For example, if the numbers length is set to '4', than 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 in combination 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.

1.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 devices from booting. When enabled, each time a new target device boots, if the Auto-add option is enabled, a new record is automatically cre-

ated in the database and 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, then select the Disable or Enable menu option.

> **Tip:**
>
> To disable all target devices as they are 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), then 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.

Creating vDisks

September 13, 2018

Use the information in this article to create a base vDisk image.

vDisks act as a hard disk for a target device and exist as disk image files on a Provisioning Server or on a shared storage device. A vDisk consists of a VHDX base image file, any associated properties files (.pvp), and if applicable, a chain of referenced VHDX differencing disks (.avhdx).

When creating a vDisk image file, keep the following facts 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 or NTFS 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).

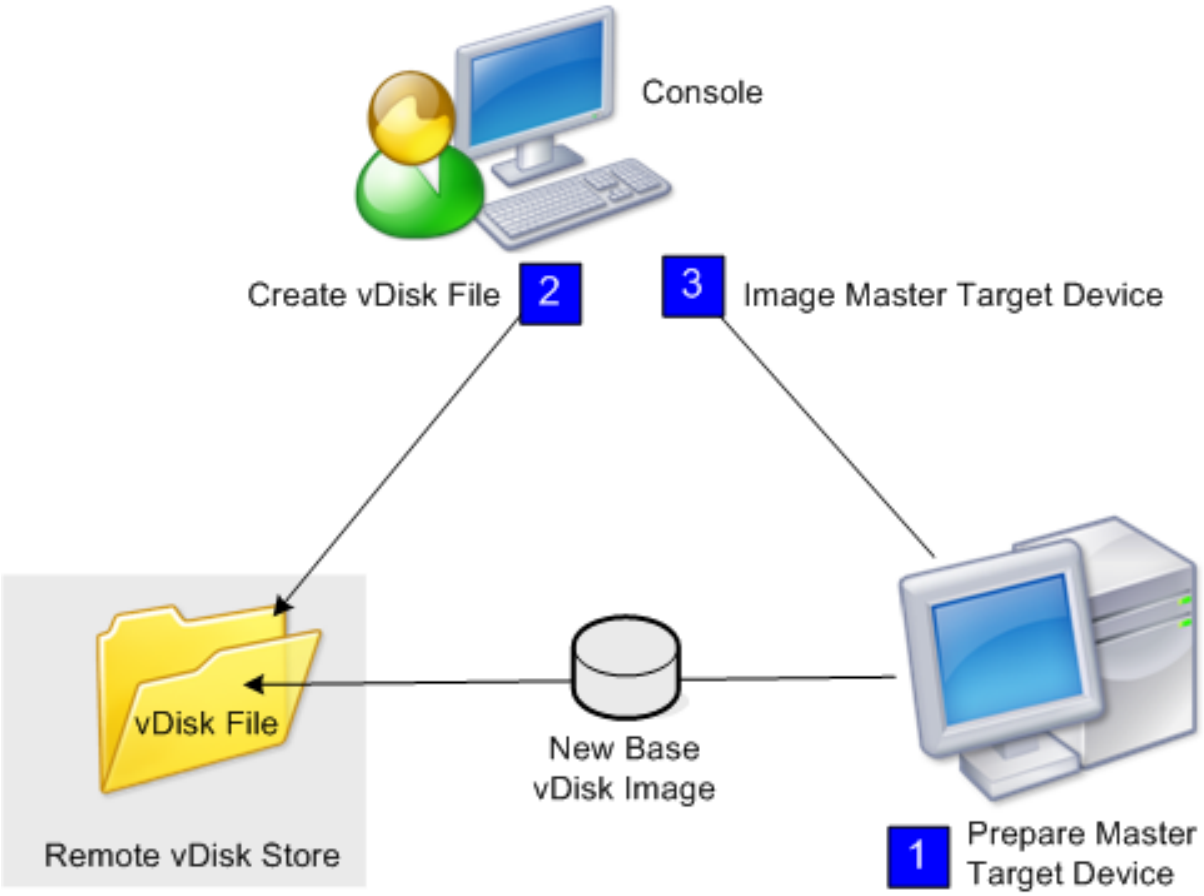
The first stage in the lifecycle of a vDisk is creating one. Creating a vDisk requires preparing the master target device for imaging. Once the image is prepared, create and configure a vDisk file where the vDisk resides. Image the master target device to that file. These steps result in a new base vDisk image. This process can be performed automatically, using the Imaging Wizard, or manually. Citrix Provisioning also provides the option to create a common image for use with a single target platform or for use with multiple target platforms.

> **Note:**
>
> Your administrator role determines what displays and which tasks you can perform in the Console. For example, you can 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 only supports automated vDisk capture. More steps require a vDisk attached to the machine being captured (which ensures that a P2PVS switch can be used with P2PVS or 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.

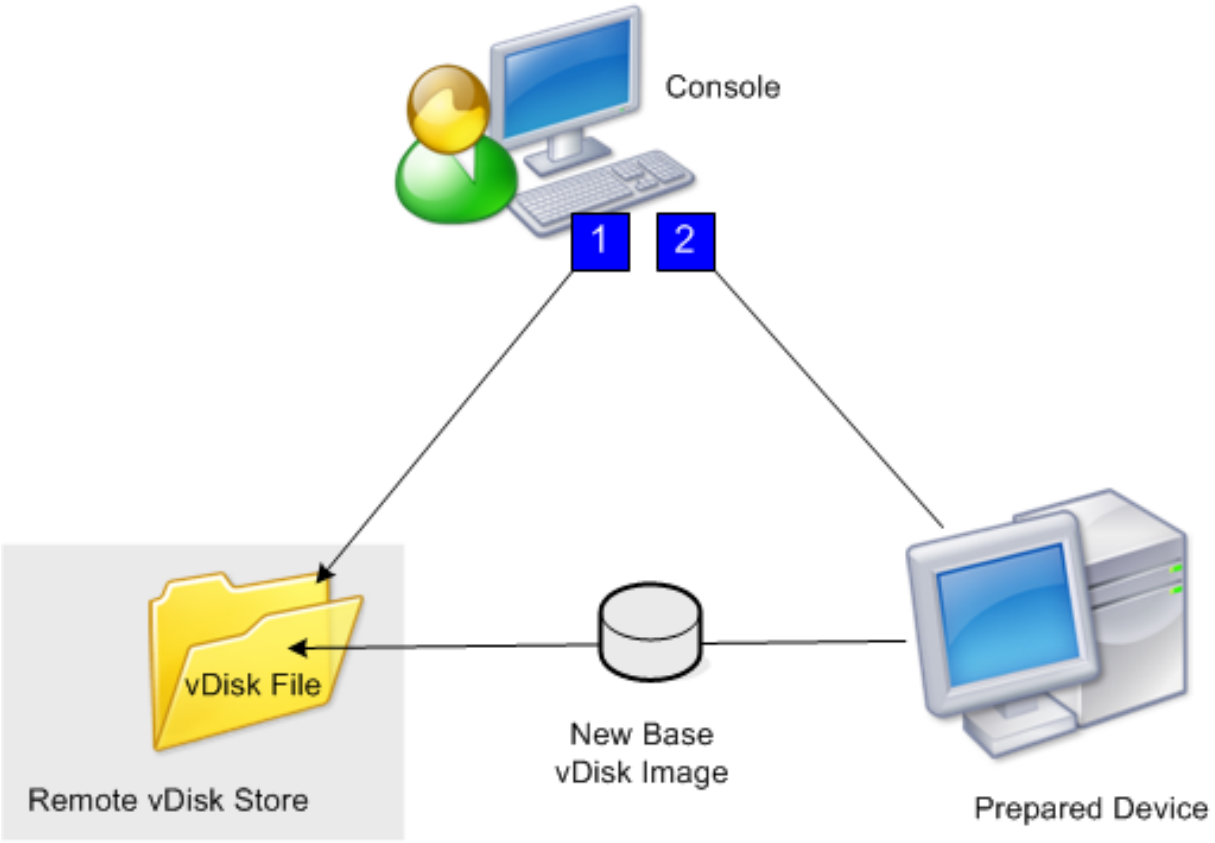


> **Note:**
>
> The master target device, physical or virtual, is prepared by installing and configuring the operating system. Also, configure applications that should be included in the base vDisk image. For details, refer to Preparing the Master Target Device.

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 Provisioning Services 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 that should be included in the base vDisk image. A vDisk file is then created on a Provisioning Server or shared storage. Access it using any Provisioning Server providing the vDisk. The file must be mounted, formatted, then unmounted manually. Accomplish this from the Console or from the target device.

   > **Note:**
   >
   > In the 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 Provisioning Services imaging utility.

   > **Note:**
   >
   > The imaging utility converts a server or desktop workload from an online physical machine running Windows to a XenServer virtual machine or provisioned vDisk. The imaging utility can convert 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 drop-down menu, select the store where this vDisk should reside. If you accessed this dialog from the store, from the drop-down menu, select the site where this vDisk is added.
3. In the Server used to create the vDisk drop-down menu, select the Provisioning Server that creates the vDisk.
4. Type a filename 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** drop-down, 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 may take several minutes or more to create the vDisk. After the vDisk is successfully created, it displays in the 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 Provisioning Services 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, refer to vDisks.
- Multiple types of physical devices (different motherboards, network cards, video cards, and other hardware devices). For details, refer to Creating a Common Image for use with Multiple Physical Device Types.

- Blade servers. For details, refer to 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 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 XenConvert Software

XenConvert software and installation instructions can be downloaded from either the Citrix Provisioning Services product download site or the XenServer product download site.

After successfully installing XenConvert on the target device:

1. Run XenConvert on the target device to convert the physical machine into a XenServer VM.

2. Set the VM's vCPU setting to be the same as the physical system's vCPU setting.

   > **Note:**
   >
   > This step is important for NT5 OS.

3. Change the XenServer VM MAC (it is using the physical system's MAC address of the NIC), or remove the NIC to add a new one.
4. Boot the XenServer VM.

Install XenServer tools

1. Log on to the master target device as a domain administrator, or a domain user (with local install privileges).
2. Run windows-pvdrivers-xensetup.exe, which can be downloaded from on the XenServer Product installation CD or product download site. The **Citrix XenServer** Windows Tools Setup warning dialog appears.
3. Click **Yes** to continue the install.
4. Follow the onscreen prompts and select the default settings. At the **Choose Install Location** dialog box, click **Install**.
5. When prompted by Windows Plug and Play dialogs, select the option to find drivers automatically.
6. When prompted select **Yes** for any unsigned driver dialog.
7. When prompted, reboot the master target device.
8. Verify that Citrix Provisioning successfully binds to the XenServer NIC and the physical systems NIC.

Image the Provisioning Server Master Target device

Use either the Citrix Provisioning Imaging Wizard or XenConvert to create the XenServer vDisk image. When creating the vDisk image, you must select to optimize target device settings. Otherwise the VM may fail to boot.

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, refer to Using the Imaging Wizard. For details on using XenConvert to create the XenServer vDisk image, refer to XenConvert product documentation on the Citrix Provisioning or XenServer product download site.

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 either the Citrix Provisioning Imaging Wizard or XenConvert 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 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 BIOS.

- 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. The BIOS Structure contains a list of all the components connected to the motherboard so that the appropriate drivers are loaded to allow 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, it is likely that you have not installed drivers for that target device's chipset. 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. (Recommended) Make 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 form 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 pro-

> cedure 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 **BIOS 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 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. This functionality can be used to provide a highly secure environment which allows you to configure systems so that only trusted applications can be used. Refer to the [Microsoft site] (https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization) 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:

- refer to the Microsoft documentation site to configure [Device Guard] (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control-deployment-guide).
- refer to the Microsoft documentation site to [configure nested virtualization] (https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/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.

> **Tip:**
>
> Citrix Provisioning supports Device Guard using Hyper-V 2016 with targets running Windows 10 or Windows 2016.

Configuring vDisks for Active Directory management

July 31, 2018

Integrating Citrix Provisioning and Active Directory allows administrators to:

- Select the Active Directory Organizational Unit (OU) in which Citrix Provisioning should create a target device computer account.
- Take advantage of Active Directory management features, such as delegation of control and group policies.
- Configure the 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 image optimization wizard was run during imaging.

After all prerequisites have been verified, new target devices can be added and assigned to the vDisk. A machine account must then be created for each target device.

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 Provisioning 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 re-negotiation of machine passwords. This is done by enabling the Disable machine account password changes security policy at either the domain or target-device level. Provisioning Server provides equivalent functionality through its own Automatic Password Renegotiate feature.

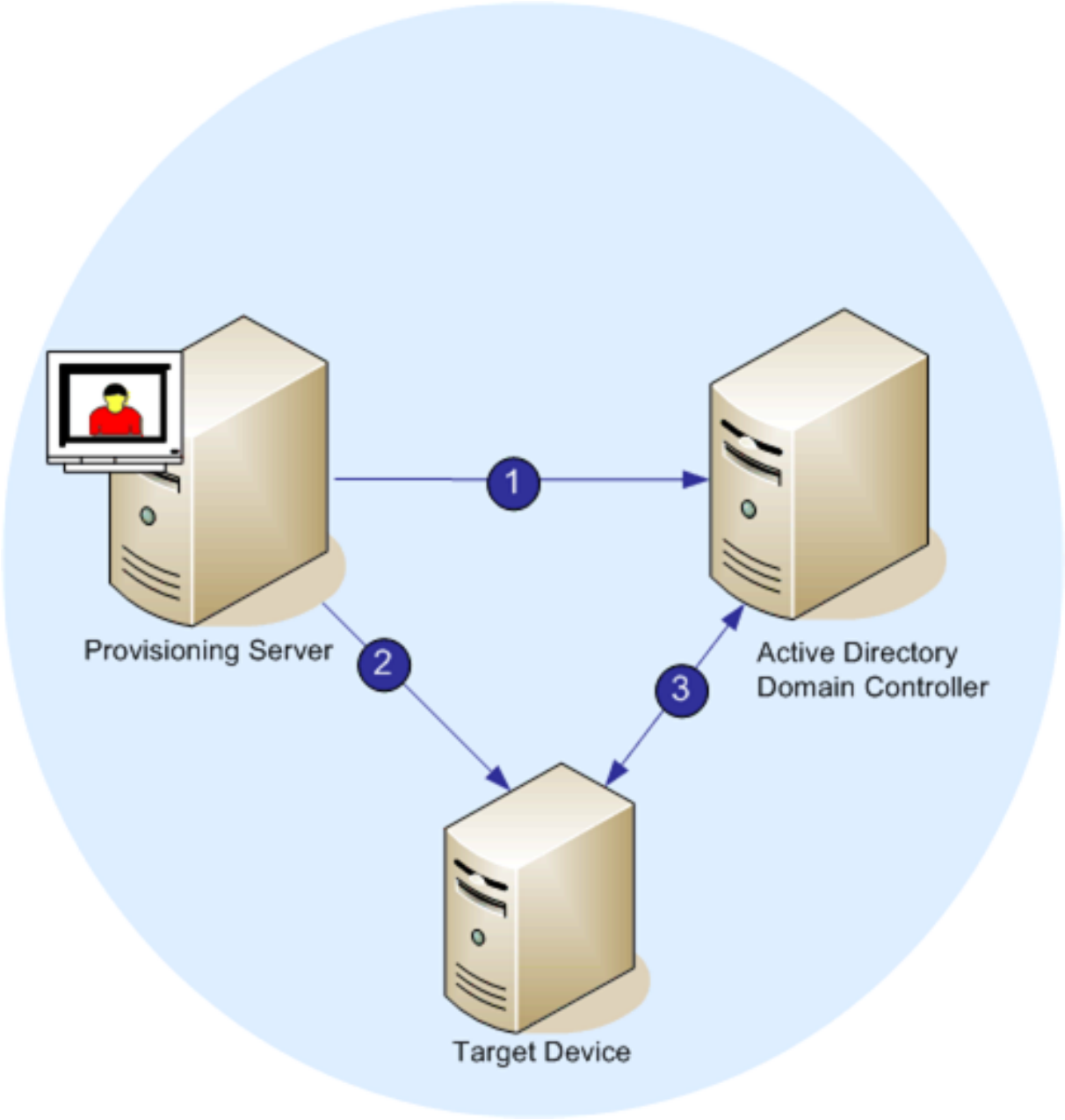
While target devices booting from vDisks no longer require Active Directory password renegotiation, configuring a policy to disable password changes at the domain level applies to any domain members booting from local hard drives. This may not be desirable. A better option is to disable machine account password changes at the local level. To do this, select the Optimize option when building a vDisk image. The setting will then be applied to any target devices that boot from the shared vDisk image.

> **Note:**
>
> The Provisioning Server does not in any way change or extend the Active Directory schema. 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 that is 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 can not 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 Console, then select theFile Properties menu option.
2. On the Options tab, select Active Directory machine account password management.
3. Click OK, then close the properties dialogs, then restart the Streaming Service.

Enabling automatic password management

If your target devices belong to an Active Directory domain and are sharing a vDisk, the following additional steps must be completed.

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 Provisioning Server, rather than in Active Directory, in order to take full advantage of product features.

Supporting cross-forest scenarios

To support cross-forest scenarios:

- Ensure that DNS is properly set up. (Refer to 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. In order for Citrix Provisioning and the user from that domain 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

A common cross-domain configuration involves having the Provisioning Server in a parent domain and users from one or more child domains who want to 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 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 into the Provisioning Server as the child domain user.

Cross-forest configuration

This configuration is similar to the cross-domain scenario, except that the Provisioning Services Console, user, and Citrix Provisioning 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 new accounts in the OUs.

Giving access to users from another domain Provisioning Services administrator privileges

Citrix recommends the following method:

1. Add the user to a Universal Group in their own domain (not the Citrix Provisioning Domain).

2. Add that Universal Group to a Local Domain Group in the Citrix Provisioning domain.
3. Make that Local Domain Group the Citrix Provisioning Admin group.

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 (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 Active Directory Management dialog appears.
2. From the Domain scroll list, select the domain that the target device(s) belongs to, or in the Domain Controller text box, type the name of the domain controller that the target devices should be added to (if you leave the text box blank, the first Domain Controller found is used).
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 the Add devices button to add the selected target devices to the domain and domain controller. A status message displays to indicate if each target device was added successfully. 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 Management, then select Delete machine account. The Active Directory Management dialog appears.
2. In the Target Device table, highlight those target devices that should be removed from the domain, then click the Delete Devices button. 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 Management, then select Reset machine account. The Active Directory Management dialog appears.

2. In the Target Device table, highlight those target devices that should be reset, then click the Reset devices button.

   > **Note:**
   >
   > This target device should have been added to your domain while preparing the first target device.

3. Click Close to exit the dialog.
4. Disable Windows Active Directory automatic password re-negotiation. To do this, 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 be logged on with 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.

Assigning vDisks to target devices

August 15, 2018

A vDisk can be assigned 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 vDisks displays 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 refer to Accessing a vDisk Version. Maintenance and Test devices with non-production versions are labeled appropriately.

A vDisk cannot be assigned to a target device using drag-and-drop if that target device was assigned a personal vDisks using the XenDesktop Wizard. A message dialog displays if a vDisk is dragged and dropped onto a collection containing one or more target devices using personal vDisks. The dialog provides the option to continue by acknowledging that the vDisk is assigned to those devices that are not currently assigned a personal vDisk. Also, target devices using personal vDisks cannot inherit the

properties of a target device that fail to use a personal vDisk (copy/paste). To reassign a vDisk to a target device that uses a personal vDisk, see Configure target devices that use personal vDisks.

Assigning vDisks to a target device

vDisks can be assigned to a single target device using:

- Drag-and-drop
- Target Device Properties dialog

To assign a vDisk, using drag-and-drop, to one or all target devices within a collection:

1. In the 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 and drop 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 Console tree, expand the Device Collections folder, then click on 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 should use from the Boot from drop-down 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.

Using the Streamed VM Setup Wizard

August 24, 2018

The Citrix Provisioning Streamed VM Setup Wizard helps with deploying a streamed vDisk to several cloned virtual machines (VMs).

Use the wizard to:

- Create VMs on a supported hosted hypervisor from an existing template:
  - XenServer

  - Hyper-V via SCVMM
  - ESX via V-Center
- Create Citrix Provisioning target devices within a Collection
- Assign a vDisk 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 vDisk in Standard Image mode exists, to be 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 XenServer, 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 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 present 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 Provisioning Services:
  - 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 vDisk 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 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 convenient reuse, the most recently used hypervisor and username is cached in the registry of the local machine running this instance of the 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 vDisk 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. Enable the radio button next to one of the following methods used for adding Active Directory computer accounts, 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.

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** drop-down box, then select from the OUs listed for that Domain.
- In the **Account naming scheme** drop-down box, select a valid naming scheme consisting of at least one hash symbol (#) that is 15 characters or less. Additionally, select a number/character fill option that dynamically replace 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 appear in 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. If the wizard fails or is canceled in the middle of an operation, any progress made is retained. If cleanup of existing progress is required, it must be done 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. Names associated with storage devices are retained by Citrix Virtual Apps and Desktops and 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 could 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

August 30, 2018

The Citrix Virtual Apps and Desktops Setup Wizard (XDSW) helps with deploying virtual desktops to virtual machines (VMs) as well as to devices that use personal vDisks.

> **Important:**
>
> The Provisioning server must have direct access to the storage device to facilitate communication. The Citrix Provisioning user must have read\write access to the storage device to ensure successful provisioning with the HDD BDM.

The wizard:

- Creates VMs on a Citrix Virtual Apps and Desktops-hosted hypervisor using an existing machine template:
  - XenServer
  - ESX via V-Center
  - 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. Refer to 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.
- Assigns a Standard Image vDisk 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.

> **Note:**
>
> For Citrix Virtual Apps and 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 should be aware of the new partition. For example, an RDS provisioning image using a write cache disk and BDM partition should see 2 partitions in private image mode.
>
> **Tip:**
>
> 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 vDisk through the SOAP server. For details, see Installation.

ESX permissions

For ESX 5.5, 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

> **Note:**
>
> Other previously supported versions of ESX may require the same permissions to work with Citrix Provisioning 7.x.

Write cache considerations

The Citrix Virtual Apps and Desktops Set Up Wizard discards any hard disks that are attached to a template. This process minimizes provisioning time.

The wizard provisions diskless VMs if the vDisk 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 vDisk 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 XenDesktop can boot the VMs as necessary.

If the write cache is stored on hypervisor local storage, configuring deployment through the XenDesktop Setup wizard varies depending on your hypervisor:

- On XenServer, VMs are spread across multiple local storage resources. Create the template without storage (network boot).
- On Hyper-V, VMs are spread across multiple local storage resources. The configuration file follows the write cache, but it is a small file.
- On ESX, you cannot use the XenDesktop 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 (,). Names associated with storage devices are retained by Citrix Virtual Apps and Desktops and 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.

Virtual disk types

VMs provisioned through the XenDesktop 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 XenServer
- "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.

1. Right-click on any Site icon in the **Console** tree panel, then select the Citrix Virtual Apps and Desktops Setup Wizard…menu option. The Citrix Virtual Apps and Desktops Setup Wizard appears.
2. Click **Next** to begin setup.
3. On the Citrix Virtual Apps and Desktops Host page, enter the location of the Citrix Virtual Apps and Desktops Host address to connect to and to configure. The most recently used Citrix Virtual Apps and Desktops Controller (name or IP) is cached in the registry of the local machine running this instance of the Console.
4. Select a **XenDesktop 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 (Username and Password).
6. 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, a page displays so you can select the appropriate network.
8. Select a single Standard Image mode vDisk 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. Provides the option to save a user's changes to a Personal vDisk.
        - Windows Server Operating System – best for delivering hosted shared desktops for a large-scale deployment of standardized machines or applications, or both.
        - The vGPU option only is supported only on desktop operating systems.
    - If you select an existing catalog using the drop-down menu, that catalog's description, machine type, assignment type, and user data (if applicable) display.
10. Select **VM preferences**. Preferences vary depending on the machine OS type and whether or not assigned user changes are discarded after the session ends.
    a) For Windows Client or Windows Server machines that are randomly assigned to users who do not require a personal vDisk:
        - Number of VMs to create (default is 1)
        - vCPUs (default is based on the previously selected template)
        - If the template has dynamic memory configured, two extra configuration settings are required (minimum and maximum memory).
        - Local write cache disk (default is 6 GB)
        - Boot mode; PXE boot (requires a running PXE service). BDM disk (creates a partition for the Boot Device Manager file).

b) For Windows Client machines that are either randomly assigned or statically assigned to users who can save their changes to their personal vDisk, in addition to the preferences listed above, the following preferences display:
   - Personal vDisk size (default is 10 GB). When booting a target device from a personal vDisk, the vDisk's OS partition, C:\ by default, only shows the amount of space allocated to the personal vDisk. It does not display the true size of the personal vDisk.
   - Personal vDisk drive letter (default is P). The drive letter the target device uses for the personal vDisk. The range allowed is between E: to U: and W: to Z:.

11. Choose the appropriate method for adding Active Directory computer accounts:
    - Create accounts
    - Import existing accounts

    The page that displays depends on which Active Directory method you select.

12. To Create new accounts: Delegate rights to the Provisioning Console user to allow Active Directory account creation or modification to manage computer account passwords.
    - Select the appropriate domain from the **Domain** drop-down box, then select from the OUs listed for that domain. The domain and OU default to rights of the current user.
    - Select the machine-naming option from the Account naming scheme drop-down text box. Enter a valid naming scheme consisting of at least one hash symbol (#) that is 15 characters or less. Additionally, 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.

13. To Import existing accounts:
    - 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. 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. They do not display in the list. Citrix Virtual Apps and Desktops (as a machine), Citrix Provisioning (as a device), and on the hypervisor (as a VM). If the AD structure contains many objects or containers, or if you are importing a large amount of machine accounts, the import may take a while. It must validate that each imported account does not exist in Citrix Provisioning, Citrix Virtual Apps and Desktops, and the destination hypervisor. If so, you should receive feedback in the form of an hour glass cursor while the import completes.

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 XenDesktop catalog
    - Create VMs on a host's hypervisor using the machine template
    - Create BDM partitions, if specified
    - If using a Streamed with personal vDisk Catalog, create a personal vDisk, then attach the personal vDisk to the VM
    - Create a write cache disk of the specified size
    - Create Citrix Provisioning target devices then assign the selected vDisk to those devices
    - Add the target devices to the selected Provisioning Services Collection
    - Add the VMs to the XenDesktop catalog
    - Boot each VM to format the newly created write cache disk

If you cancel during the configuration, you must manually remove the following:

- XenDesktop machines from the assigned catalog
- Active Directory computer accounts that were created.
- Newly created XenDesktop catalogs.
- Citrix Provisioning target devices created in the selected device collection.
- VMs created on any of the selected host hypervisors.

vDisks can be updated and reassigned to a target device that uses personal vDisks. However, the base disk must be of the same operating system and must have the machine SID. To accomplish this, copy the target device's currently assigned base vDisk image, update the image to include new Citrix Provisioning software and drivers. Reassign the updated vDisk to the target device. To reassign the vDisk, use the vDisk Properties Assign vDisk dialog on the Console.

Nutanix Acropolis requirements

The following are required when using Citrix Provisioning with Nutanix Acropolis:

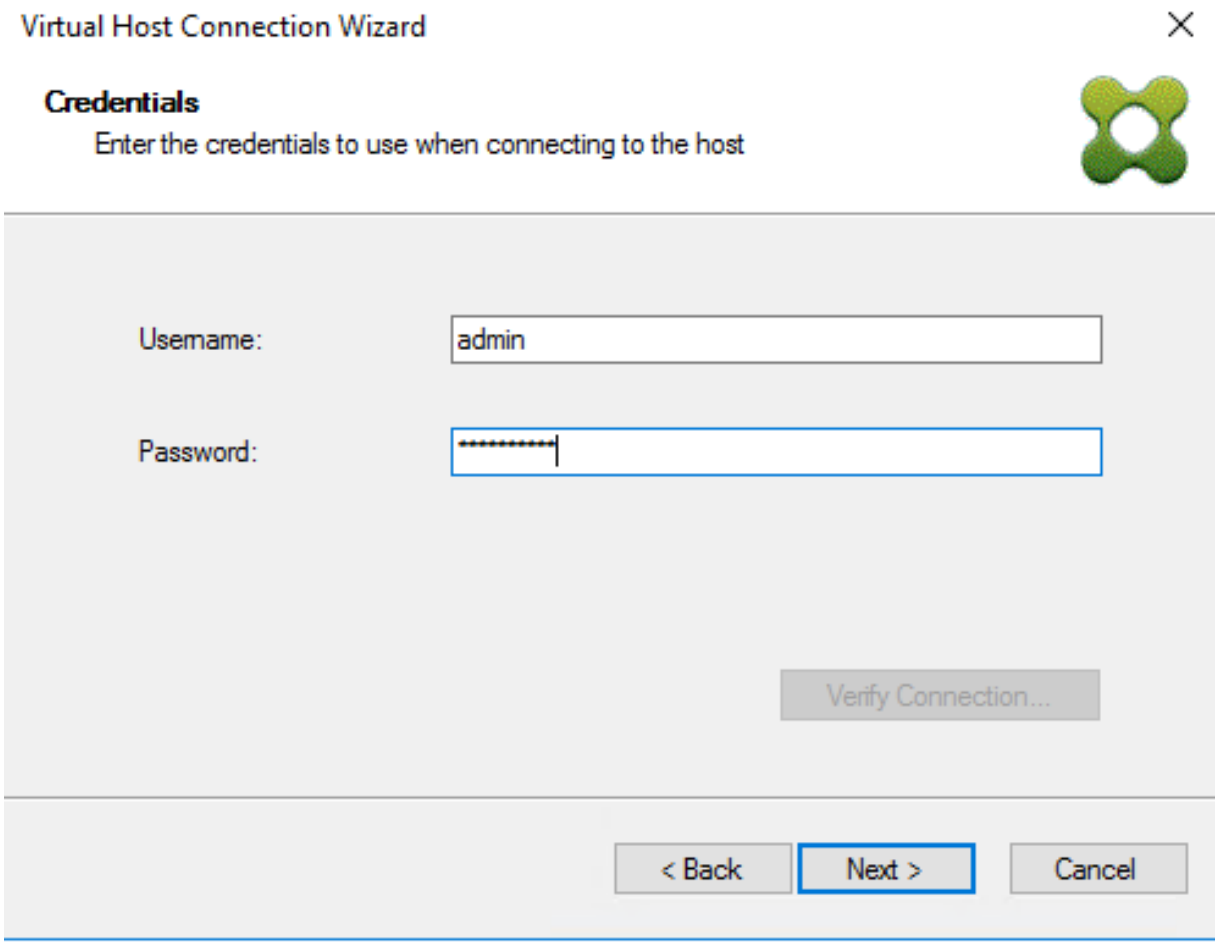
- An installed Nutanix Acropolis hypervisor plugin for PVS. Download this plugin from the Nutanix support site. Refer to the Nutanix documentation site for installation information.
- A XenDesktop host connection to AHV.
- Nutanix Acropolis platform version 5.1.1 or greater.

> **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.
- Linux VMs, BDM partitions, and UEFI are not supported.
- Only the XenDesktop Setup Wizard is supported, not the Streamed VM Wizard.
- Acropolis hypervisors use snapshots and not templates for VMs.
- It's considered best practice that a snapshot does not have an attached hard disk because the Nutanix Acropolis hypervisor does not remove the hard disk during provisioning.
- To deploy machines that boot from BDM ISOs, the ISO should be mounted in the snapshot. The provisioned VMs are set to use PXE boot and must be manually changed to boot from virtual optical drive.
- For PXE booting, you must use a command line option to set the VM boot order to *network* before imaging.
- When manually adding a Nutanix AHV host using the Virtual Host Connection Wizard, not enough information exists to effectively communicate with the Nutanix AHV hosting unit. This information, provided by the Citrix Virtual Apps and Desktops DDC, is not shared with the Virtual Host Connection Wizard. As a result, this information is not used to verify credentials. Therefore, the **Verify Connection** button in the Virtual Host Connection Wizard is disabled for Nutanix AHV hosts.



> **Note:**
>
> For information related to the configuration and use of Nutanix Acropolis hypervisors, see the Nutanix documentation portal.

SCVMM requirements

You cannot provision vGPU-enabled VMs on Hyper-V.

Provisioning vGPU-enabled Citrix Virtual Apps and Desktop machines

August 30, 2018

Requirements

- NVIDIA GRID K1 or K2 cards.

> **Tip**
>
> Sometimes, other NVIDIA cards may function properly (for example, NVIDIA Tesla M60) as long as the XenServer/ESX hypervisor supports it. The underlying vGPU card in the XenServer host is unknown to Citrix Provisioning. Citrix Provisioning only uses the vGPU setting in the template and propagates it to the VMs provisioned by the Citrix Virtual Apps and Desktops Setup Wizard.

- A server capable of hosting XenServer and NVIDIA GRID cards.
- A supported hypervisor: Citrix XenServer 6.2 or newer, or vSphere 6.0 or newer.
- The NVIDIA GRID vGPU package for your hypervisor.
- NVIDIA drivers for Windows 7 32-bit/64-bit.
- The Citrix Provisioning release that corresponds to the Citrix Virtual Apps and Desktop release you are using. This Wizard only works with the corresponding Citrix Virtual Apps and Desktops controller.
- To provision machines using the Citrix Provisioning Setup Wizard, you must use Citrix Provisioning 7.7 or newer and XenDesktop 7.7 or newer. If you use earlier product versions you can only provision machines manually or by using the Citrix Provisioning Streamed Virtual Machine Setup Wizard.

> **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 vDisk image. If you plan to use the Citrix Virtual Apps and Desktops Setup Wizard to provision machines, select the **Target Device Optimizer** option, otherwise the VM fails to boot.

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 Provisioning Services database with the MAC address of the template VM.
3. Assign the vDisk to the template VM, and then set the device to boot from vDisk.
4. PXE boot the VM.
5. Format the write-cache disk.

Install the Citrix Virtual Apps and Desktops Virtual Delivery Agent

1. Using the Provisioning Console, set the vDisk 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 vDisk 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 Provisioning Console, set the vDisk image mode to Standard Image.
2. Choose the preferred write cache method.
3. Select from the following provisioning methods:

- Run the Citrix Provisioning Citrix Virtual Apps and Desktops Setup Wizard to provision VMs. This method is available only if you are using Citrix Provisioning 7.7 or later and XenDesktop 7.7 or later.
- Run the Citrix Provisioning Streamed VM Setup Wizard to provision VMs.
- Manually create VMs by creating target device records using device MAC addresses, assign the vDisk to the VMs, and then add the target devices to Active Directory.

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.

Virtual and blade server machine catalogs	Steps
Requirements: For Citrix Virtual Apps and Desktops, the host record must point to the XenServer host or pool where the vGPU VMs existed. The VM names in your hypervisor, device record names in **Citrix Provisioning device** collection, and the Active Directory record must all be the same.	1). Start the Citrix Virtual Apps and Desktops Machine Catalog Setup Wizard. Select **Windows Desktop OS** on the **Operating System** page. 2). On the **Machine Management** page, for ”This Machine Catalog uses&quot, select Machines that are power managed. 3). For **Deploy machines using** select **Citrix Provisioning**. Power management is 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). In the structures that appears, select the **Citrix Provisioning device** collection where all the vGPU devices are located, then click **Next**. Device records should be stored in an exclusive device collection. 7). In the structures that appears, select the **Provisioning device** collection where all the vGPU devices are located, then click **Next**. Device records should be stored in an exclusive device collection, 8). Enter a machine catalog name and description, then click **Finish**.

Physical machine catalogs	Steps
Requirements: Device names must exist in **Citrix Provisioning device** collection and in Active Directory. **Note:** 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. On the **Machine Management** page, for **This Machine Catalog uses** select Machines that are not power managed (for example, physical machines). 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 structures that appears, select the **Citrix Provisioning device** collection where all the vGPU devices are located, and then click **Next**. Device records should be 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, refer to the Citrix Virtual Apps and Desktops documentation.

Citrix Provisioning and Citrix Virtual Apps and Desktops cloud considerations

Within a Cloud DDC, you can create a machine catalog and choose to deploy those machines using Citrix Provisioning by pointing the catalog to a **Provisioning** collection. If you intend to use Citrix Provisioning with a Cloud DDC, all the machines within the Provisioning collection must be associated with Active Directory (AD) accounts.

Citrix Provisioning Accelerator

August 27, 2018

Citrix Provisoning Accelerator enables a provisioning proxy to reside in Dom0 (the XenServer Control Domain) on a XenServer host where streaming of a provisioning vDisk is cached at the proxy before being forwarded to the VM. Using the cache, subsequent booting (or any IO requests) of the VM on the same host can be 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.

With this functionality:

- Citrix Provisioning and XenServer provide an improved functional paradigm by providing a unique value available when used together.
- Citrix Provisioning provides support for local, NAS, and SAN attached storage in XenServer.
- Environments experience reduced network traffic.
- Deployments experience improved fault tolerance, with tolerance for outage instances of a Provisioning Server.

> **Important:**
>
> This feature is only supported on XenServer version 7.1 (or later) with the proxy capability installed. UI changes only occur when you are using that type of hypervisor. To use this feature, an optional package must be installed on the XenServer host. There are no additional dependencies on the installer.
>
> For more information on the relationship between XenServer and Citrix Provisioning, refer to the blog XenServer and Citrix Provisioning: Better Together.
>
> **Tip:**
>
> Citrix recommends that you do not disable this feature on a VM using the XenServer console. When disabled using this method, Citrix 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 the sections *Enabling or disabling Citrix Provisioning Accelerator for individual devices* and *Enabling or disabling Citrix Provisioning Accelerator for all devices on a host* later in this article.

Using Citrix Provisioning Accelerator

The proxy feature is only supported on XenServer with the proxy capability installed (version 7.1). UI changes only occur when you are using that type of hypervisor. An optional package must be installed on the XenServer host. There are no additional dependencies on the installer.

Before using this feature the XenServer administrator must create a Citrix Provisioning Site object using the XenServer console. This process effectively configures the storage (that is, storage repositories) that is used when proxying the IO requests. This work must be performed on XenServer.

Consider the following when using this feature with XenServer:

- A XenServer Citrix Provisioning Site object must be created and configured with the storage repository (SR) before the Provisioning Console can establish a proxy connection on the VM.
- Citrix Provisioning calls the XenServer API to check if the proxy feature is enabled before it exposes any Provisioning/XenServer proxy interfaces.
- Citrix Provisioning configures the XenServer proxy for devices using the Citrix Virtual Apps and Desktops Setup Wizard and the Streamed VM Setup Wizard.
- Citrix Provisioning targets are aware of their proxy status. Once the feature is installed, no additional configuration tasks are required.
- 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 a one in XenCenter.

> **Tip:**
>
> In environments where two Provisioning Servers reside with the same VHD but have different file system timestamps, the data is cached twice. Due to this limitation, Citrix recommends that you use VHDX rather than VHD.

Configuring Citrix Provisioning Accelerator

Use the Citrix Virtual Apps and Desktops Setup Wizard and the Streaming Wizard to access this feature. Both Wizards are similar, and share many of the same screens. The following differences exist:

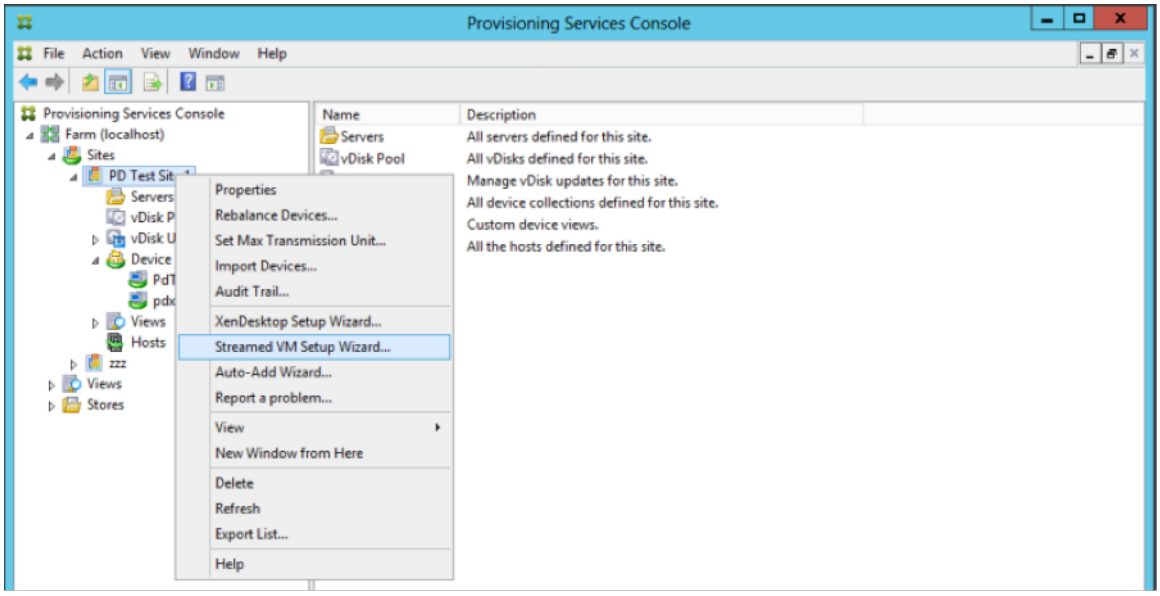
- The XenDesktop Setup Wizard is used to configure VMs running on a hypervisor (for example, XenServer, Esx, or HyperV/SCVMM) that is controlled using XenDesktop.
- The Streaming Wizard is used to create VMs on a XenServer host. It does not involve XenDesktop.

> **Note:**
>
> This feature is only supported on XenServer that has the capability installed. UI changes captured in this section only apply when you are using that type of hypervisor.
>
> **Tip:**
>
> When a proxy cache configuration (that is, Citrix Provisioning Accelerator is enabled) is tied to a Provisioning Server, and you reinstall XenServer on the host that had this feature enabled, Citrix

> Provisioning and XenServer become out of sync. This configuration occurs because the reinstallation of XenServer wipes the previously configured proxy cache configuration.
>
> 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. For this reason, the user must delete all previously configured VMs associated with this cache configuration, including the host. Reconfigure Citrix Provisioning and set up the cache again.

To configure Citrix Provisioning Accelerator, select one of the Wizards (**Citrix Virtual Apps and Desktops Setup Wizard** or **Streamed VM Setup Wizard**) in the Provisioning Console:

1. Navigate to a site.
2. Select the site, then right-click to expose a contextual menu:



1. Select the appropriate Wizard based on how you intend to use the accelerator feature.

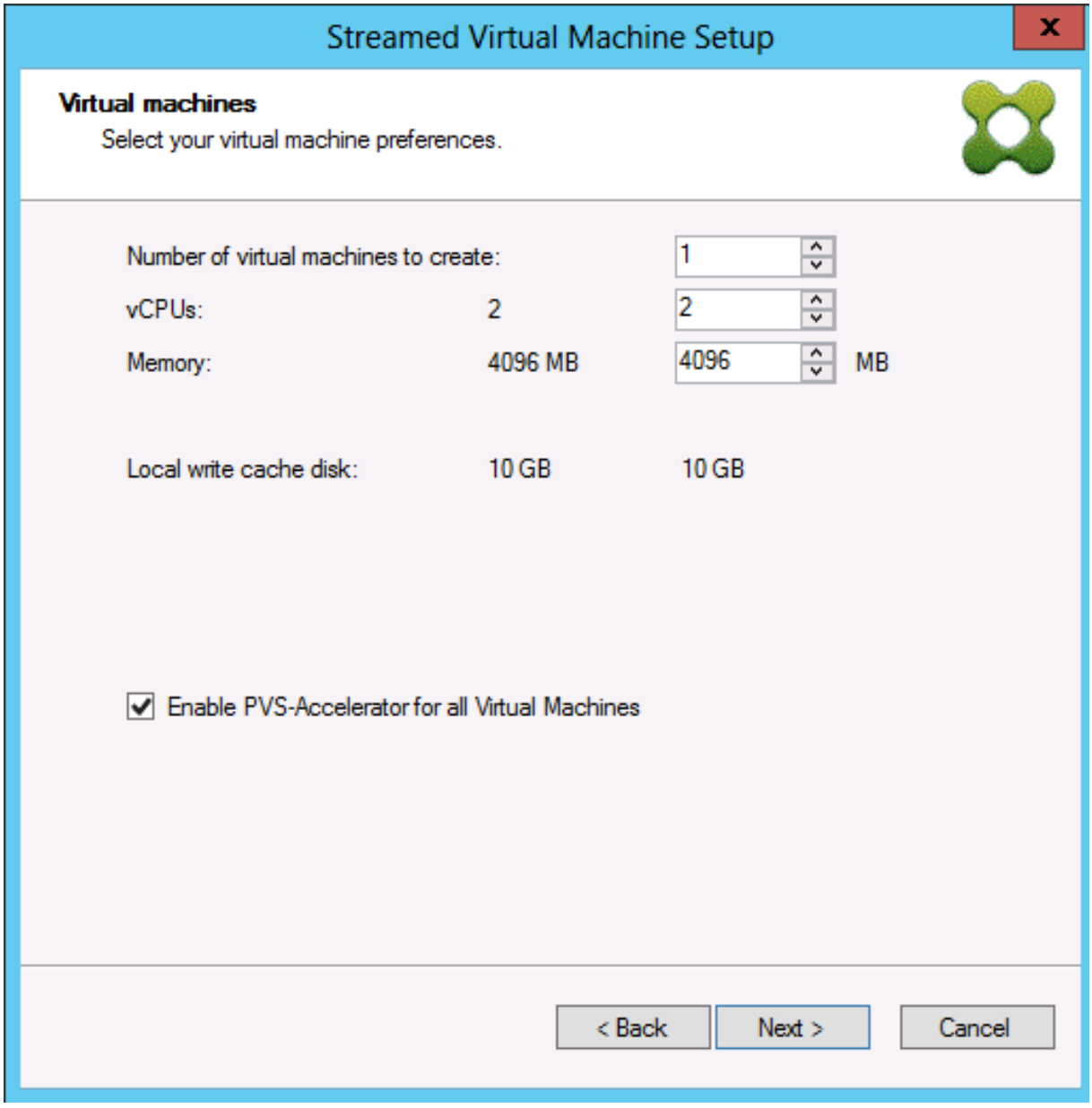
Using Wizards to configure Citrix Provisioning Accelerator

To use this feature, first determine how you use it. If you are:

- configuring VMs running on a hypervisor controlled by XenDesktop, use the **Citrix Virtual Apps and Desktops Setup Wizard**.
- creating VMs on a XenServer host that does not involve XenDesktop, use the **Streamed VM Setup Wizard**.

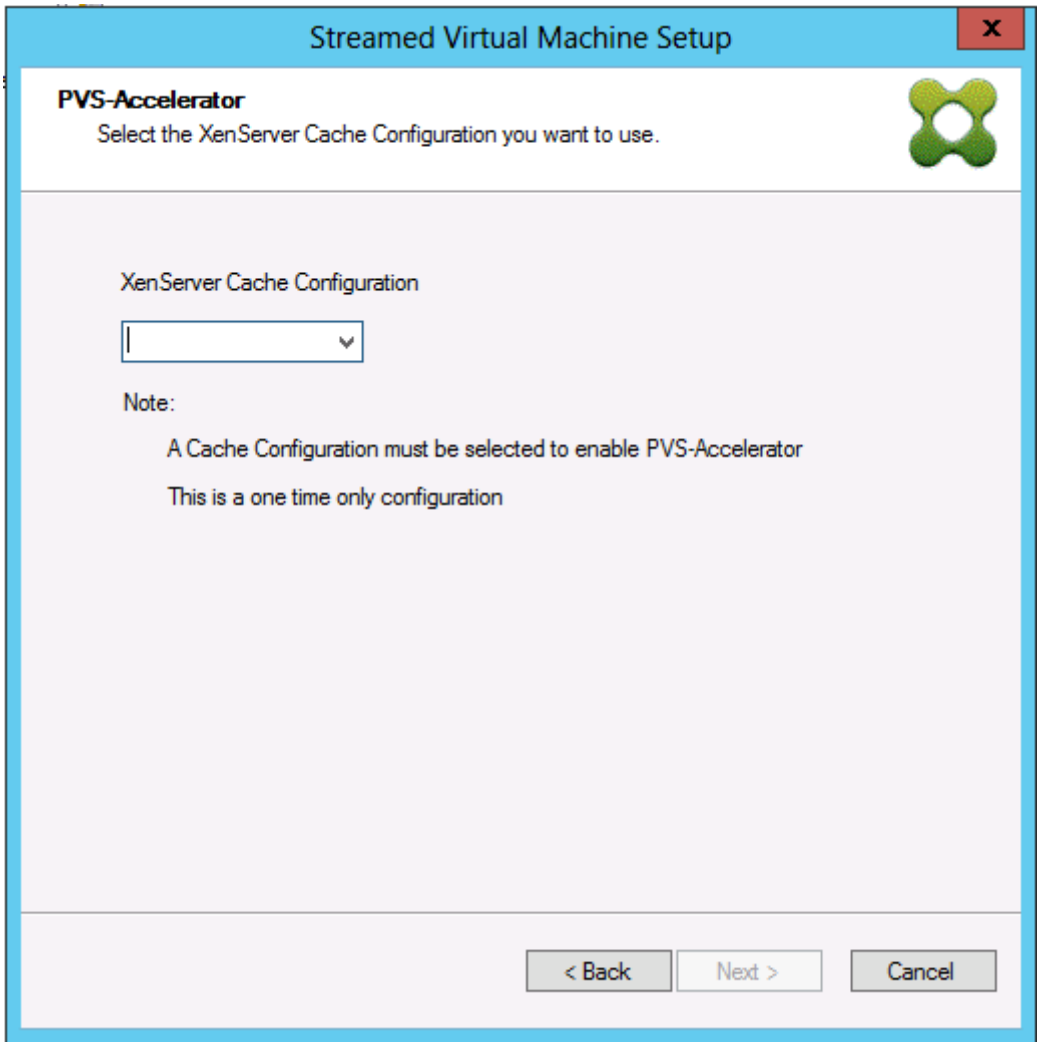
Configure proxy-accelerator using the streamed VM Setup Wizard

The Streamed Virtual Machine Setup Wizard was modified to include a new checkbox to enable the feature. After invoking the Wizard, select **Enable PVS-Accelerator for all Virtual Machines**:



> **Tip:**
>
> After selecting **Enable PVS-Accelerator for all Virtual Machines**, all VMs that are created using the Wizard are configured to use the proxy feature.

After enabling this feature, the following screen appears (the first time PVS-Accelerator is enabled for the host) after clicking **Next**:



> **Tip:**
>
> The Wizard allows you to select the XenServer Citrix Provisioning Site to which you want to apply accelerator functionality. In the XenServer screen, a drop-down list displays the list of all the Citrix Provisioning Site objects on XenServer that have been configured but not yet associated with a Provisioning site.

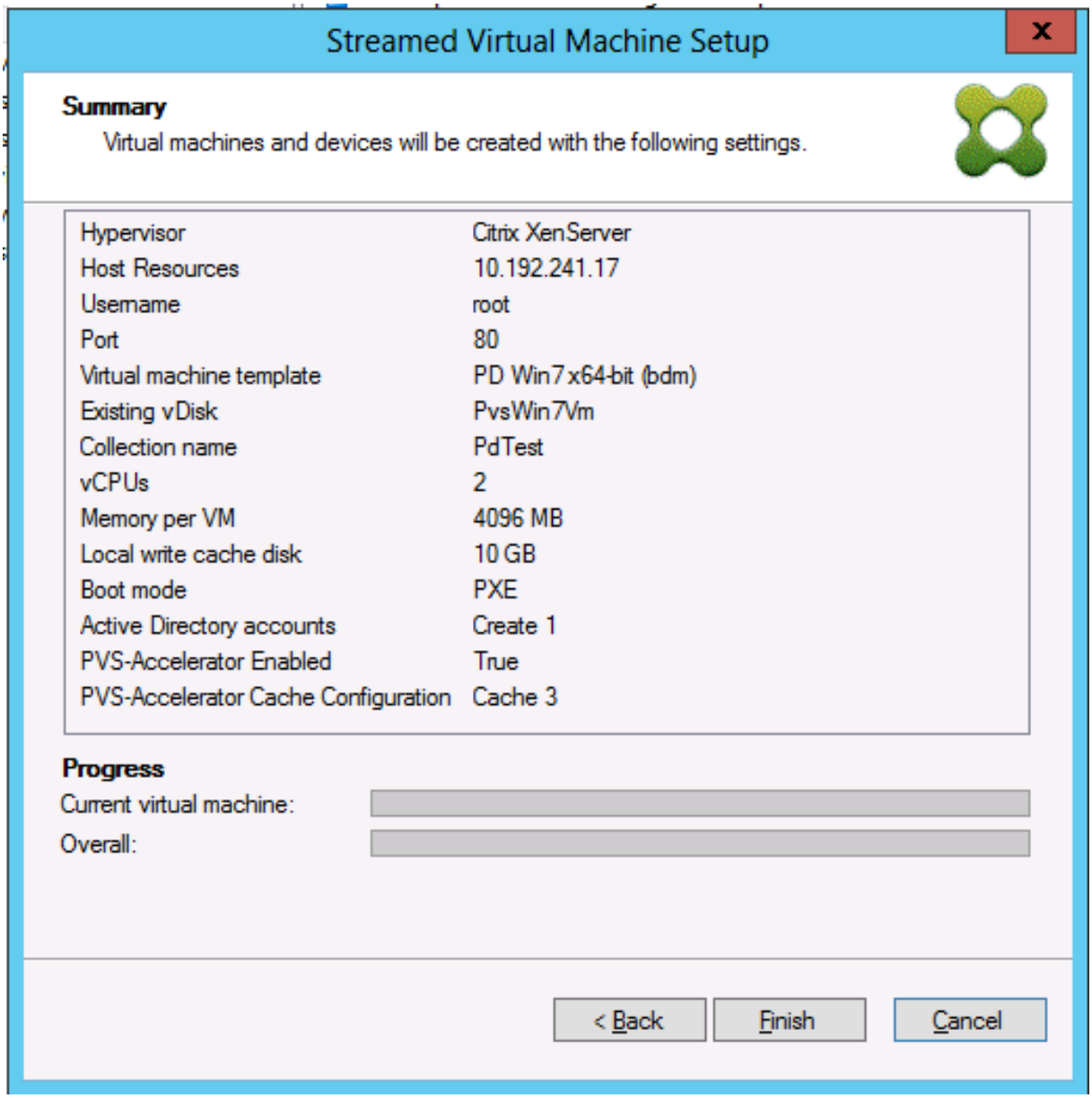
In the drop-down menu, select a Provisioning site to associate with accelerator functionality. After selecting it, the site is now associated with the Citrix Provisioning site that was selected from which to run the Wizard.

> **Note:**
>
> The next time this Wizard is run for the same Citrix Provisioning site using the same XenServer, this page is not displayed.

After using one of the Wizards to configure this feature, the Summary screen appears illustrating the current state. Use this screen to determine if it is enabled, and the current cache configuration asso-

ciated with it.

Click **Finish** to apply the configuration:

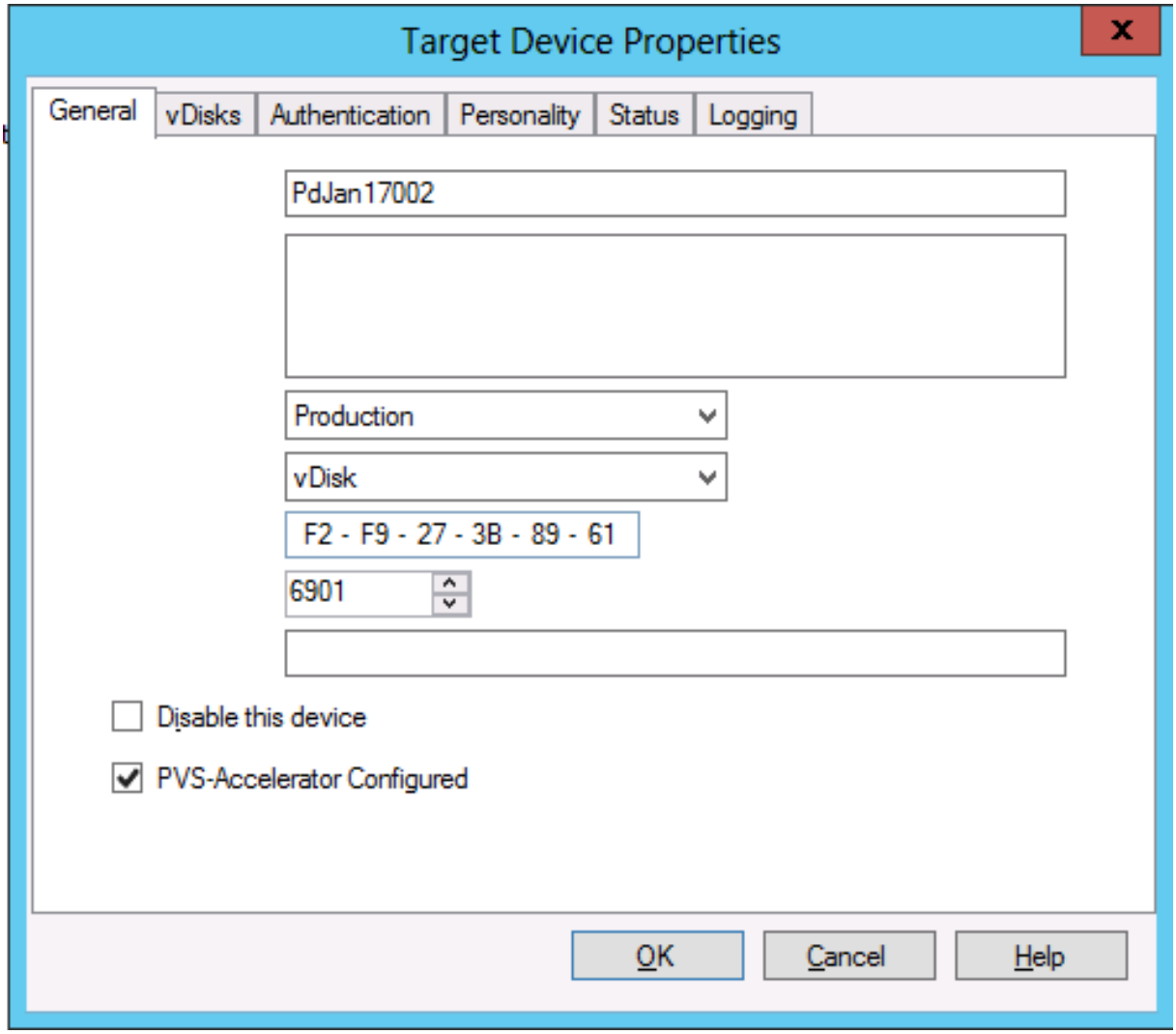


Enabling or disabling Citrix Provisioning Accelerator for individual devices

If a device was created using either Wizard (Citrix Virtual Apps and Desktops Setup Wizard or the Streaming Wizard), and Citrix Provisioning Accelerator was configured for that XenServer host in the Wizard, you can use the **Target Device Properties** screen to enable or disable the feature for an individual device.

To enable or disable this feature for an individual device:

1. Access the **Target Device Properties** screen.
2. In the **General** tab, select (or deselect) **PVS-Accelerator Configured**.
3. Click **OK** to apply the change.



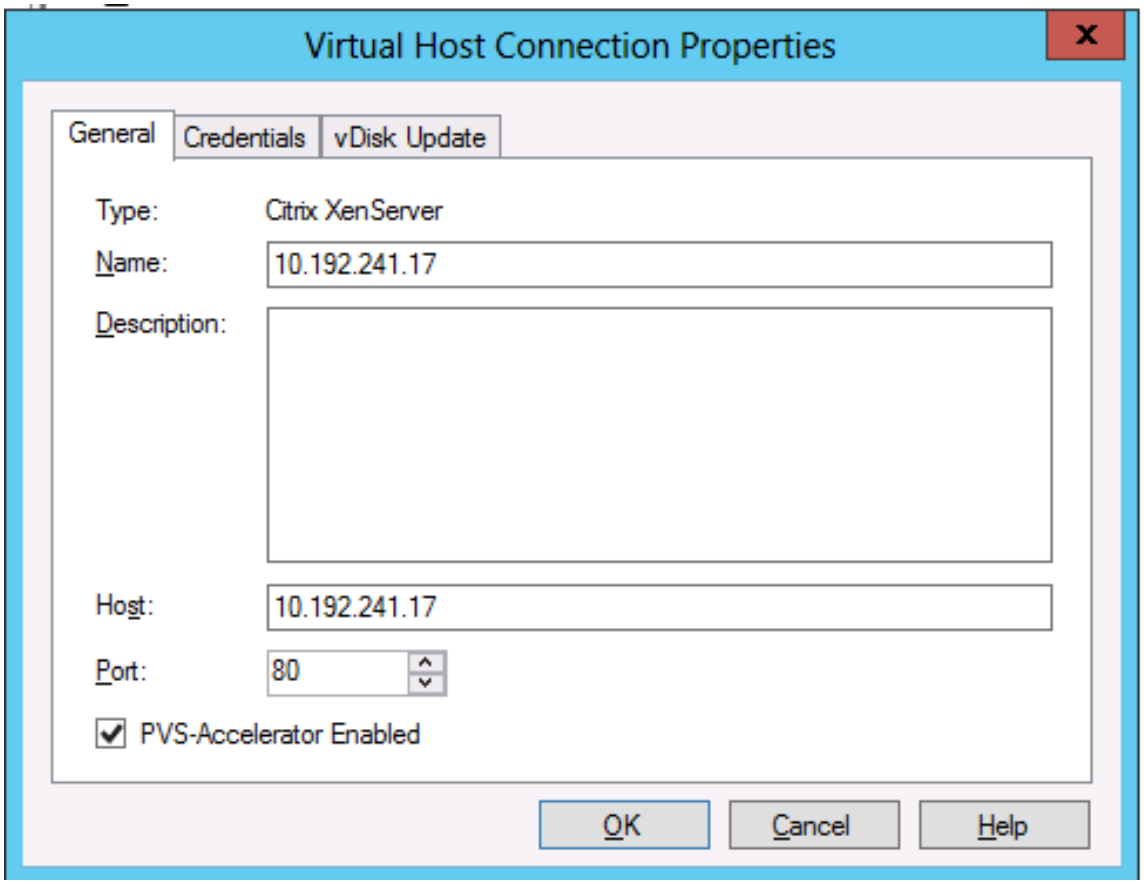
Disabling Citrix Provisioning Accelerator for all devices on a host

If this feature was enabled for a host, you can disable it using the **Virtual Host Connection Properties** screen for all devices on the specified host.

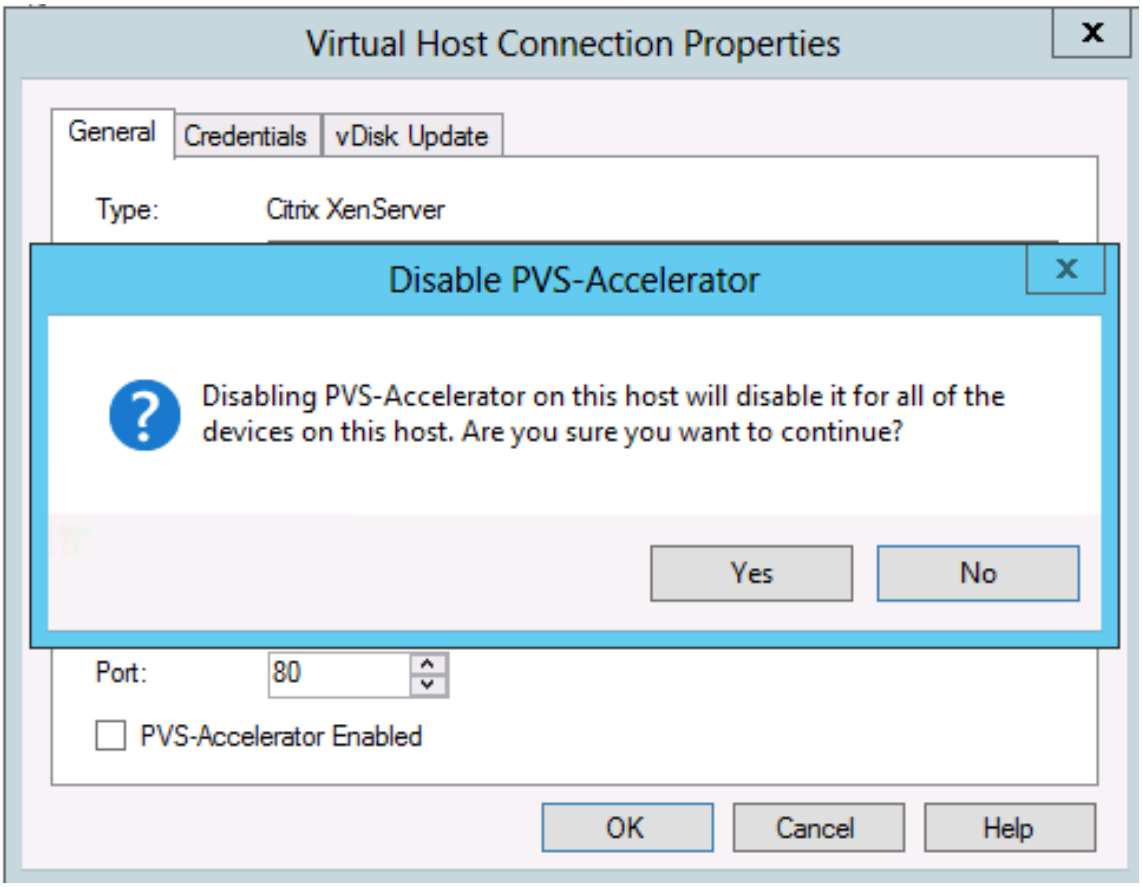
> **Important:**
>
> You cannot use the **Virtual Host Connection Properties** screen to enable PVS-Accelerator on the specified host. You must enable the feature using one of the Wizards (Citrix Virtual Apps and Desktops Setup Wizard or Streamed Wizard) while creating devices.

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. You are prompted to confirm the following action:



4. After verifying the action, click **OK** to apply the change.

UEFI pre-boot environments

September 28, 2018

Citrix Virtual Apps and Desktops supports Unified Extensible Firmware Interface (UEFI) hardware technology on Hyper-V (Generation 2) and ESX VMs. These elements are managed using SCVMM and vCenter respectively and streamed using Citrix Provisioning. This functionality enables you to:

- Stream the server operating system at startup time using gigabit network speeds, so users experience faster startups.
- Support TB disks in a virtualized environment.

UEFI is a complete replacement for the BIOS and requires a new bootstrap. Two bootstraps are available: one for 32-bit and one for 64-bit systems. The introduction of another bootstrap complicates network topologies depending upon how the bootstrap is delivered.

Network topology

Using a PXE server allows for the simplest topology because the PXE protocol works with multiple architectures. The Citrix Provisioning PXE Server recognizes the architecture flag embedded in the DHCP, then discovers and returns the appropriate bootstrap filename. Both legacy BIOS computers and UEFI computers may therefore be on the same network segment.

If DHCP option 67 is chosen, there are two topology options:

- On a single segment, use DHCP reservations to specify the bootstrap filename (option 67) for every target device. This process is feasible for smaller environments but quickly scales out of hand for enterprise environments.
- 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 cannot have embedded settings. DHCP options are therefore used to configure the UEFI bootstrap.

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 Services server. You can specify more than four addresses. The UEFI bootstrap reads all addresses then uses round-robin to select one address to connect to.

> **Note:**
>
> Option 17 takes precedence over option 11.

DHCP Option 17 – Root Path

The Root Path option is typically used with iSCSI to specify the server and virtual disk to start. Provisioning Services uses the following format to specify the server address:

```
pvs:[IPv4]<:17:6910>

pvs  -  Required identifier

IPv4  -  Address of a streaming NIC on the Provisioning Services server

17  -  Protocol identifier for UDP (required if a logon port is
   specified)
```



```
8
9  port  -  Logon port (not required if the default port of 6910 is used)
```

Examples:

```
1  pvs:[server.corp.com]:17:6910
2
3  pvs:[server.corp.com]
4
5  pvs:[192.168.1.1]
6
7  pvs:[192.168.1.1]:17:6910
```

Associating a target device with a bootstrap

Use the BOOTPTAB file to associate a target device with a specific bootstrap. The following issues apply to the format of the BOOTPTAB file to support mixed legacy and UEFI environment:

- The 'ar' tag specifies the architecture of the target device's boot environment. You can make multiple entries for the same MAC address but different architectures. This is useful for hardware supporting both legacy BIOS and UEFI booting.
- Wildcards are not supported. If an entry for a given MAC address is not found in the BOOTPTAB file, a default value is used.

The following table lists the architectures for BOOTPTAB:

Value	Architecture	Bootstrap file name
0	x86 BIOS	ardbp32.bin
6	x86 UEFI	pvsnbpia32.efi
7	x64 UEFI	pvsnbpx64.efi
9	EBC (for VMware ESX)	pvsnbpx64.efi

The full list of architectures is available from the IETF.

The format of the BOOTPTAB file is:

```
<hostname>:ha=<mac_address>:ar=<architecture>:bf=<bootstrap_name>
```

Examples:

```
host001:ha=001122334455:ar=0:bf=ardbp32.bin
```



```
host002:ha=554433221100:ar=7:bf=pvsnbpx64.efi
```

If the architecture flag is missing, 0 is the default value.

Citrix Provisioning managed by Citrix Cloud

September 18, 2018

Citrix Provisioning supports a connector for Citrix Cloud integration. It enables provisioned VDAs to be used in the Citrix Virtual Apps and Desktops. This connector provides the same functionality used in on-premises deployments.

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 Virtual Apps and Desktops builds a version of the Citrix Provisioning PowerShell snap-in (Citrix.PVS.snapin) with a subset of the Citrix Provisioning on-premises cmdlet. This version is built specifically to run in Citrix Cloud and communicate with Citrix Provisioning on-premises through the Citrix Cloud Connector.
- **Citrix Cloud Connector located on-premises:** The Cloud Connector acts as a relay which exposes the Azure Provisioning Service endpoints to enable communication between the Citrix Virtual Apps and Desktops Delivery Controller. Also, the Cloud Connector contains a WCF endpoint listening on the Azure Service Bus for communicating with the Provisioning Server.
- **Provisioning Server located on-premises; this server must be version 7.18 or later:** The Provisioning Server communicates with the Cloud Connector while establishing SOAP calls to MAPI.
- **Citrix Virtual Apps and Desktops Remote PowerShell SDK:** The Provisioning Console installation includes the Citrix Virtual Apps and Desktops SDK. This SDK is replaced by the Citrix Virtual Apps and Desktops Remote PowerShell SDK. The SDK is used by the Citrix Virtual Apps and Desktops Setup Wizard to push VDA records to the Delivery Controller in Citrix Cloud.
- **The Licensing Server must be on-premises:** For Citrix Provisioning deployments, the Citrix License Server must be on-premises.

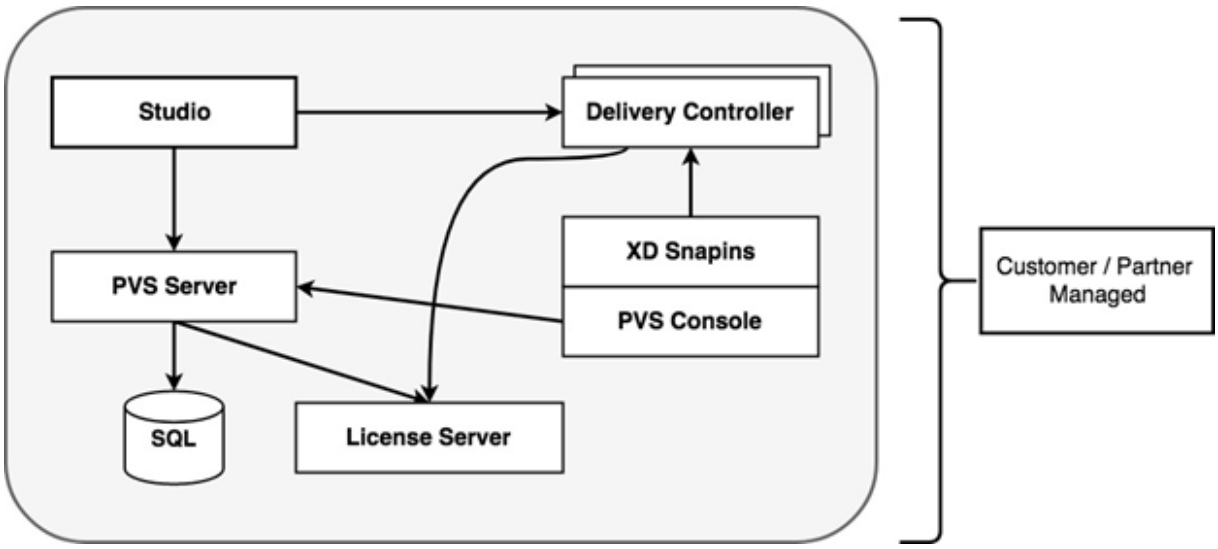
Dependencies

The following dependencies exist when using Citrix Provisioning and Citrix Cloud:

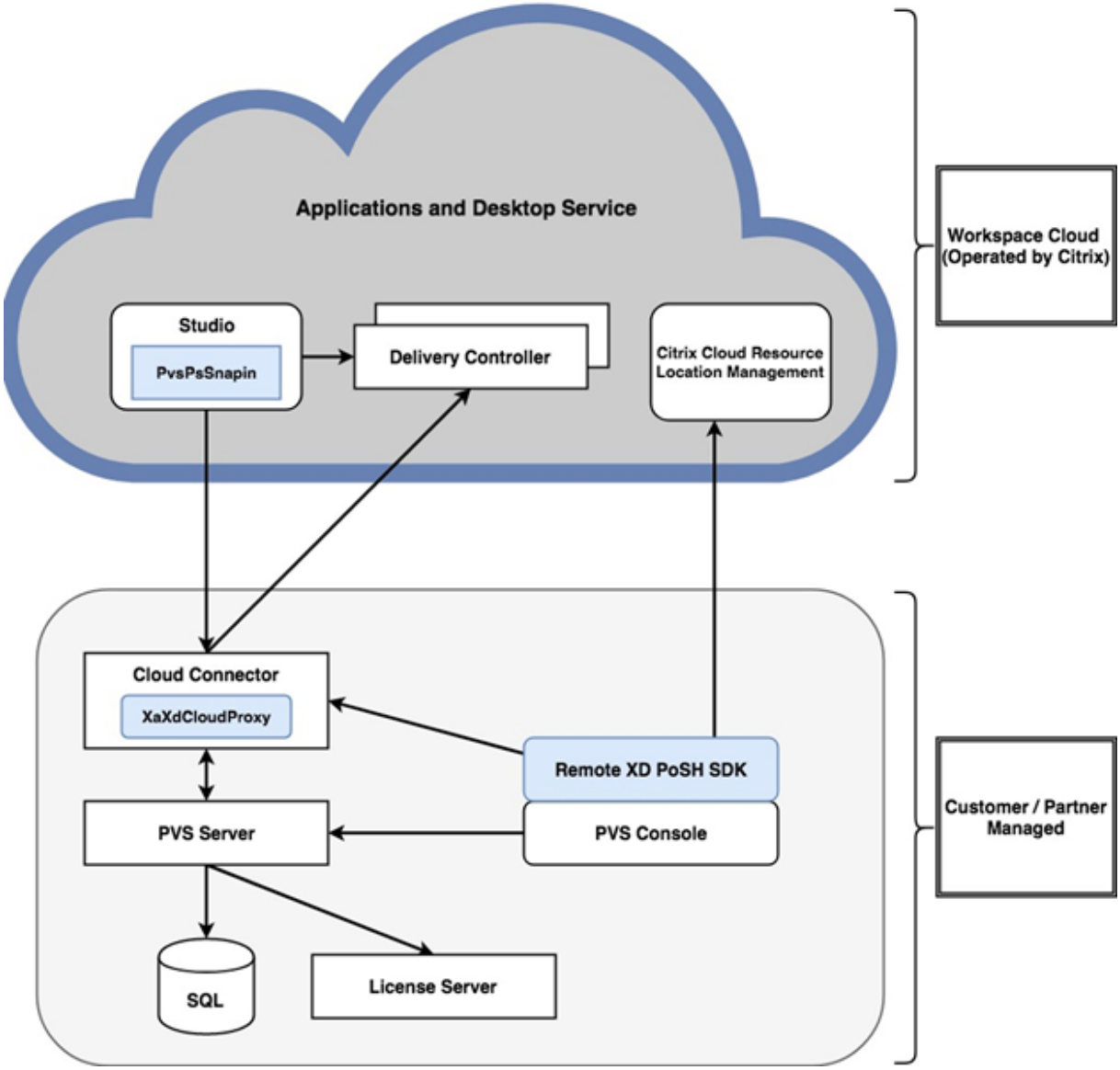
- Citrix Studio
- Citrix Cloud Connector, with the Remote Broker Provider (XaXdCloudProxy)
- Citrix Virtual Apps and Desktops Remote PowerShell SDK

On-premises versus Citrix Cloud deployments

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 to work with an on-premises Citrix Provisioning deployment:



By extending the Citrix Virtual Apps and Desktops deployment, Citrix eliminates the need to operate and manage the deployment while still providing the benefits of a managed Citrix Provisioning deployment.

Citrix Provisioning can add provisioning managed VDAs to a machine catalog in the Citrix Virtual Apps and Desktops Delivery Controller located in Citrix Cloud. This process uses one of two methods:

- Add new devices using the Citrix Virtual Apps and Desktops Setup Wizard in the Provisioning Console.
- Import existing Citrix Provisioning devices using the machine catalog creation wizard in Studio.

Citrix Virtual Apps and Desktops Setup Wizard in the Citrix Provisioning Console

The Citrix Virtual Apps and Desktops Setup Wizard (XDSW) enables you to create Citrix Provisioning devices and collections, and then create machine catalogs containing these elements. For this functionality to work with the Delivery Controller in Citrix Cloud, the Citrix Virtual Apps and Desktops SDK must be replaced with the Citrix Virtual Apps and Desktops Remote PowerShell SDK. This Remote PowerShell SDK is responsible for communicating with the Delivery Controller.

Machine catalog setup wizard using Studio

The machine catalog setup wizard imports existing provisioned-managed VMs to a Citrix Virtual Apps and Desktops catalog. In cases such as these, the VMs must be previously created using the Provisioning Console. Consider:

- Studio uses the PowerShell snap-in PvsPsSnapin to communicate with the Provisioning Server. The PvsPsSnapin is a subset of the existing Citrix Provisioning PowerShell snap-in, Citrix.PVS.Snapin. It contains the following cmdlets:
- Clear-PvsConnection
- Get-PvsVersion
- Get-SimplePvsADAccount
- Get-SimplePvsCollection
- Get-SimplePvsDevice
- Get-SimpleDiskLocator
- Get-SimpleDiskUpdateDevice
- Get-SimplePvsSite
- Get-SimplePvsUpdateTask
- Set-PvsConnection

> **Note:**
>
> In Citrix Cloud, PvsPsSnapin has been extended to enable communication from the Citrix Virtual Apps and Desktops to the PvsMapiProxyPlugin, a newly created proxy added to the XaXdCloudProxy in the Cloud Connector.

Communication is over a secure channel, HTTPS port 443, including Citrix Provisioning administrator credentials. These credentials are used by the proxy to impersonate the administrator before contacting the Provisioning Server.

Connecting your Citrix Provisioning deployment to the Citrix Virtual Apps and Desktops in Citrix Cloud

To connect an existing Citrix Provisioning deployment to Citrix Cloud:

1. Add a Cloud Connector to your managed components, for example, resource locations.
2. Upgrade Citrix Provisioning; you must use the latest version. Refer to the download page.
3. Replace the Citrix Virtual Apps and Desktops SDK on your Provisioning Console with the Citrix Virtual Apps and Desktops Remote PowerShell SDK.

   When installing this SDK, consider that the Provisioning Console on which this functionality is installed does not communicate with local Citrix Virtual Apps and Desktops deployments. This functionality also applies to the Provisioning Server. Communication exists only to the Citrix Cloud. All devices managed by the Delivery Controller in Citrix Cloud has their vDisk images and VDAs updated to use the Delivery Controller to register with Citrix Virtual Apps and Desktops.

> **Important:**
>
> An on-premises Citrix license server is required in the Citrix Virtual Apps and Desktops Service deployment. Refer to the Licensing page for more information.

Adding the Citrix Cloud Connector

Connecting a Citrix Provisioning deployment to the service requires the addition of the Cloud Connector to your managed components, for example, your resource location. When adding this connector to managed components, consider:

- The Cloud Connector installs on any domain-joined Windows 2012 R2 machine and Windows Server 2016.
- The service does not directly call into the Cloud Connector.

To add the Cloud Connector, refer to the instructions on the Citrix Cloud Connector 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. For optimum performance, Citrix recommends using Citrix Provisioning version 7.18 or later. Access the Applications and Desktops Service Downloads page for the appropriate version.

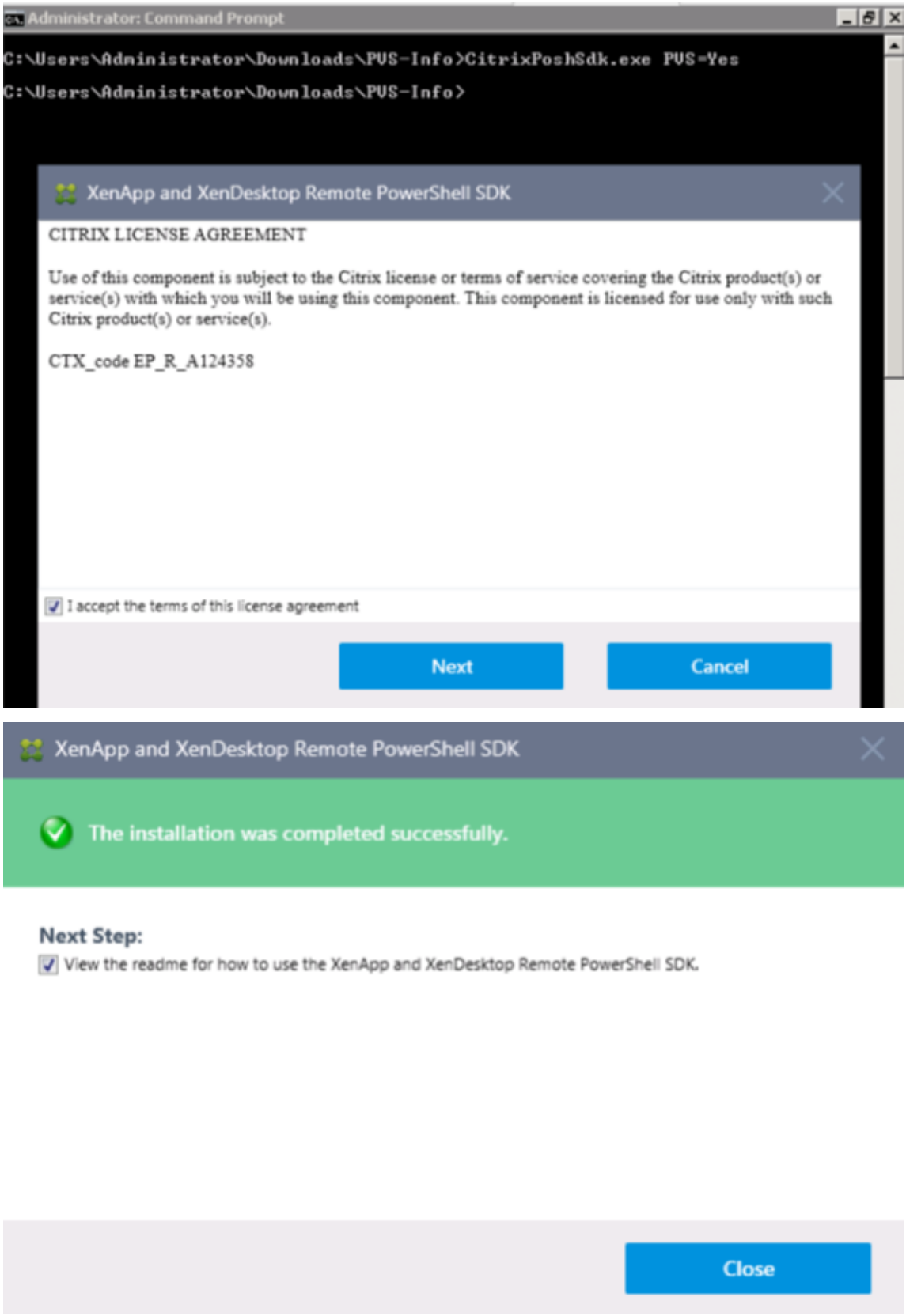
Using the Citrix Virtual Apps and Desktops remote PowerShell SDK

The Provisioning Console component includes the Citrix Virtual Apps and Desktops SDK; this SDK must be replaced with the Citrix Virtual Apps and Desktops Remote PowerShell SDK.

To use the new SDK

1. Uninstall the Citrix Virtual Apps and Desktops SDK from the Provisioning Console by removing the following snap-ins:
    - Citrix Broker PowerShell snap-in
    - Citrix Configuration Logging Service PowerShell snap-in
    - Citrix Configuration Service PowerShell snap-in
    - Citrix Delegated Administration Service PowerShell snap-in
    - Citrix Host Service PowerShell snap-in
2. Download the Remote PowerShell SDK from the Downloads page. Powershell 3.0 is required to be pre-installed.
3. Install the SDK using the command to execute: `CitrixPoshSdk.exe PVS=YES`.

    > **Important:**
    >
    > Install the downloaded SDK from the command line, and include the argument “PVS=YES.”



To verify the new SDK installation

1. Open **PowerShell**.
2. Execute the cmdlet: Add-PsSnapin Citrix*.
3. Execute the cmdlet: Get-BrokerServiceStatus.
4. Sign in to Citrix Cloud.

> **Tip:**
>
> The `Get-BrokerServiceStatus` cmdlet indicates that the Delivery Controller is **OK**.

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).
- On the Cloud Connector machine, all traffic is outbound to the cloud over HTTPS (port 443). This process enables the connector and Console to reside behind NATs and HTTP proxies.
- The new Citrix Provisioning proxy added to the Cloud Connector forwards HTTP (port 80) communications to the Provisioning Server, using wsHttp message security.

> **Note:**
>
> Personal vDisk functionality is not supported.

Administer VDAs

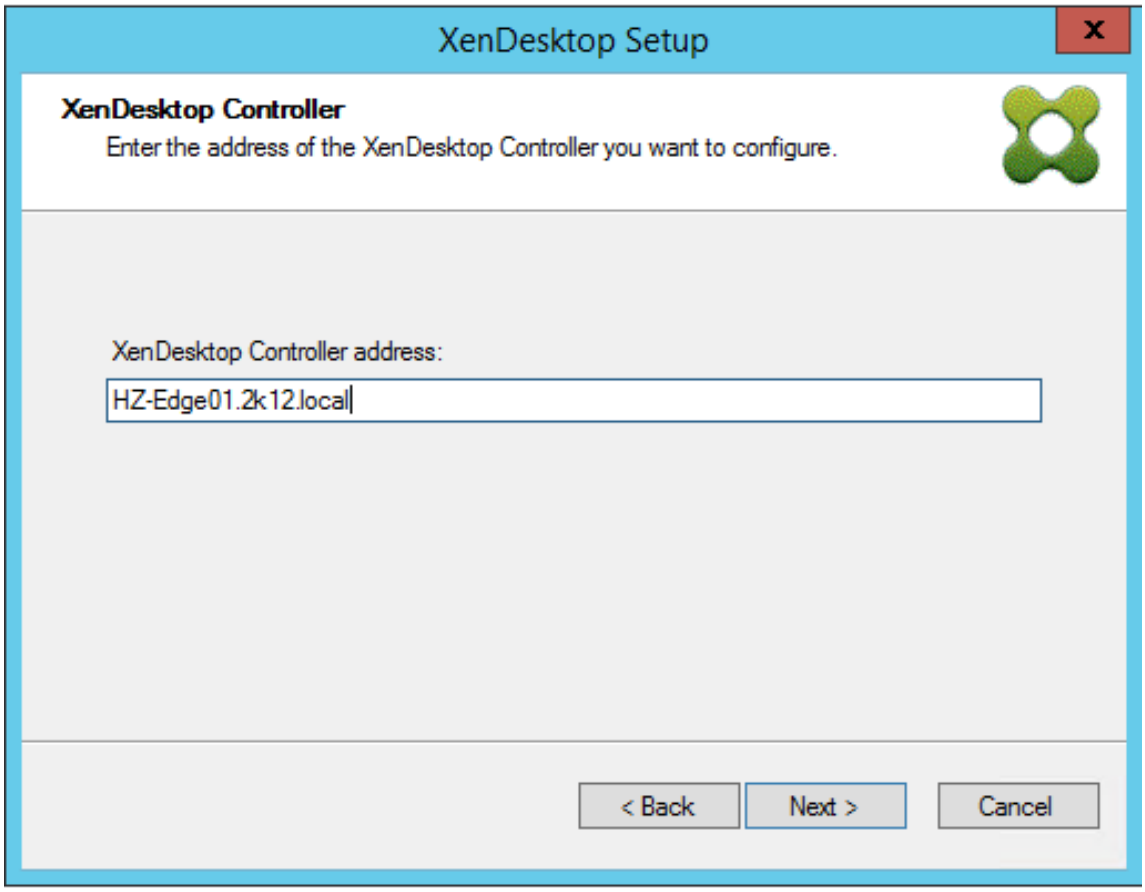
To add Citrix Provisioning managed VDAs to a machine catalog

- Use the Citrix Virtual Apps and Desktops Setup Wizard in the Provisioning Console, or;
- Use the machine catalog setup wizard in Studio

Using the Citrix Virtual Apps and Desktops Setup Wizard to add VDAs

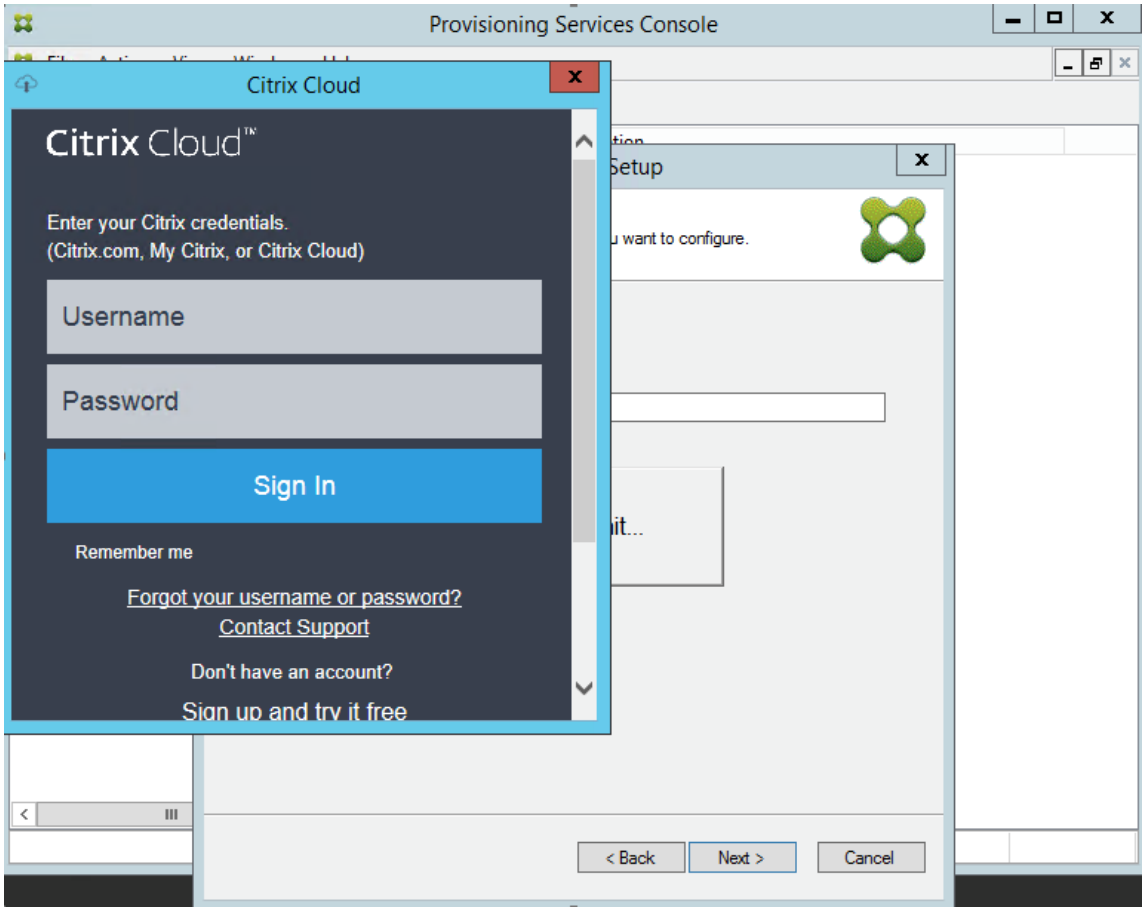
The Citrix Virtual Apps and Desktops Setup Wizard creates Citrix Provisioning devices and collections, then creates machine catalogs containing these elements. The Wizard prompts for the Citrix Virtual Apps and Desktops Controller address.

1. Provide the address of one of the Cloud Connector machines (rather than the Controller address).



2. After entering the address of the Cloud Connector, click **Next**.

   The **Citrix Cloud authentication** screen appears, prompting for sign-in credentials. This prompt, generated by the Citrix Virtual Apps and Desktops Remote PowerShell SDK, is invoked by the Provisioning Console.



> **Tip:**
>
> The Citrix Cloud credentials enable the SDK to securely communicate with the Citrix Virtual Apps and Desktops to configure the machine catalogs. The remaining steps in the Citrix Virtual Apps and Desktops Setup Wizard are unchanged. The only difference is the prompt for the Citrix Cloud sign-in credentials when the wizard first invokes the cmdlet in the Remote PowerShell SDK.

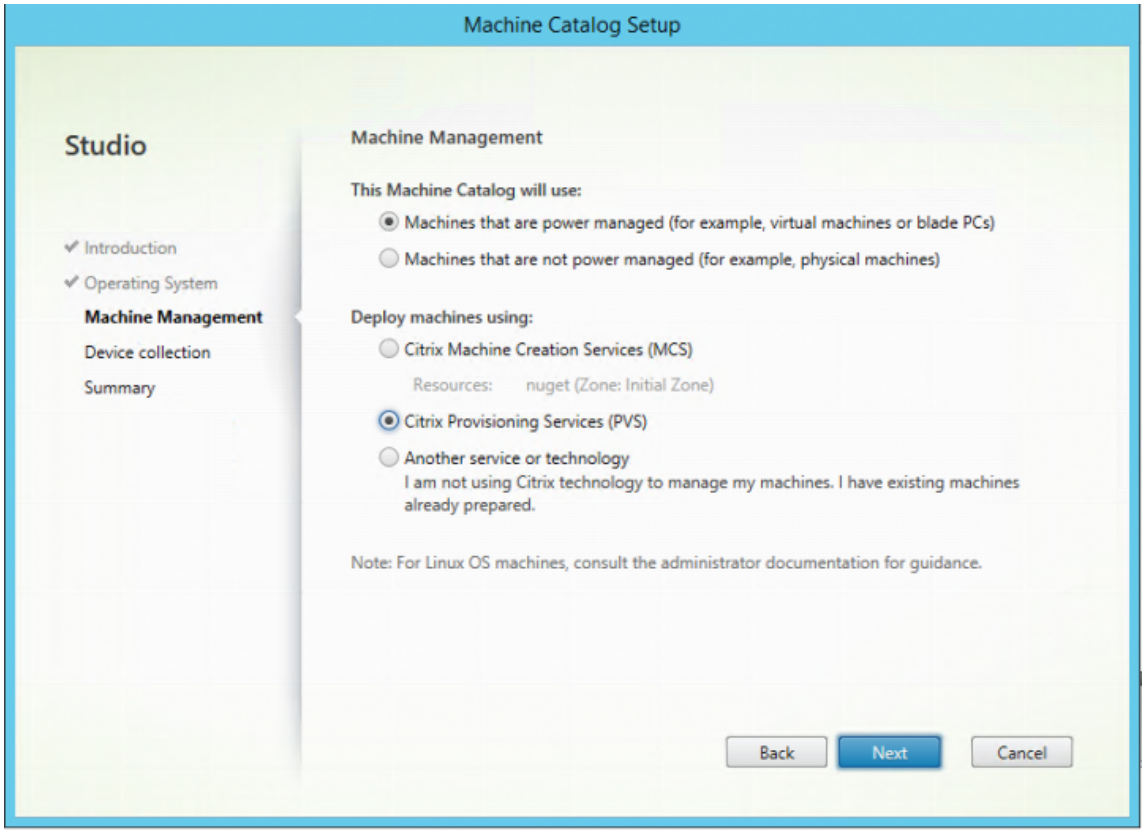
Using the machine catalog setup wizard to add VDAs

This Studio wizard adds existing managed Citrix Provisioning VMs to a catalog. In this scenario, the VMs were previously created using the Provisioning Console.

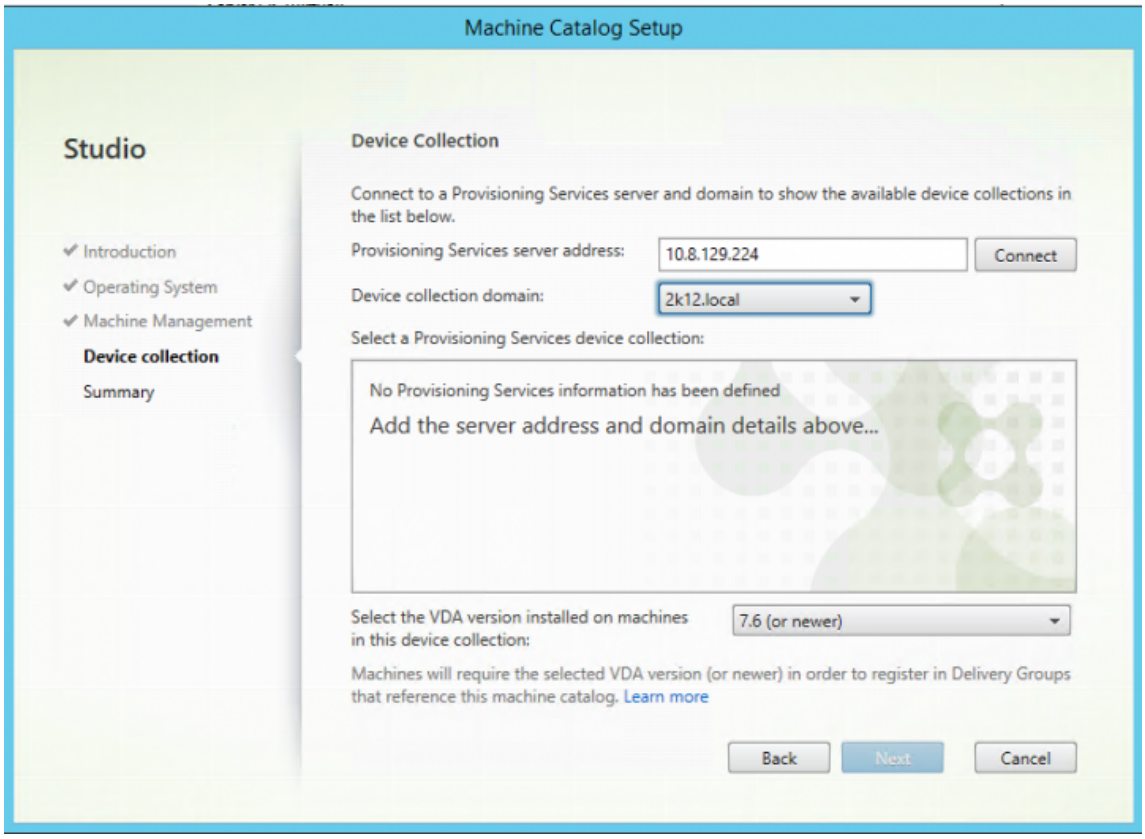
To use this wizard

1. Access Studio from the **Manage** tab of the Citrix Virtual Apps and Desktops page.
2. Select **Machine Catalogs** in the navigation pane.
3. Click **Create New Catalog** in the **Actions** pane.

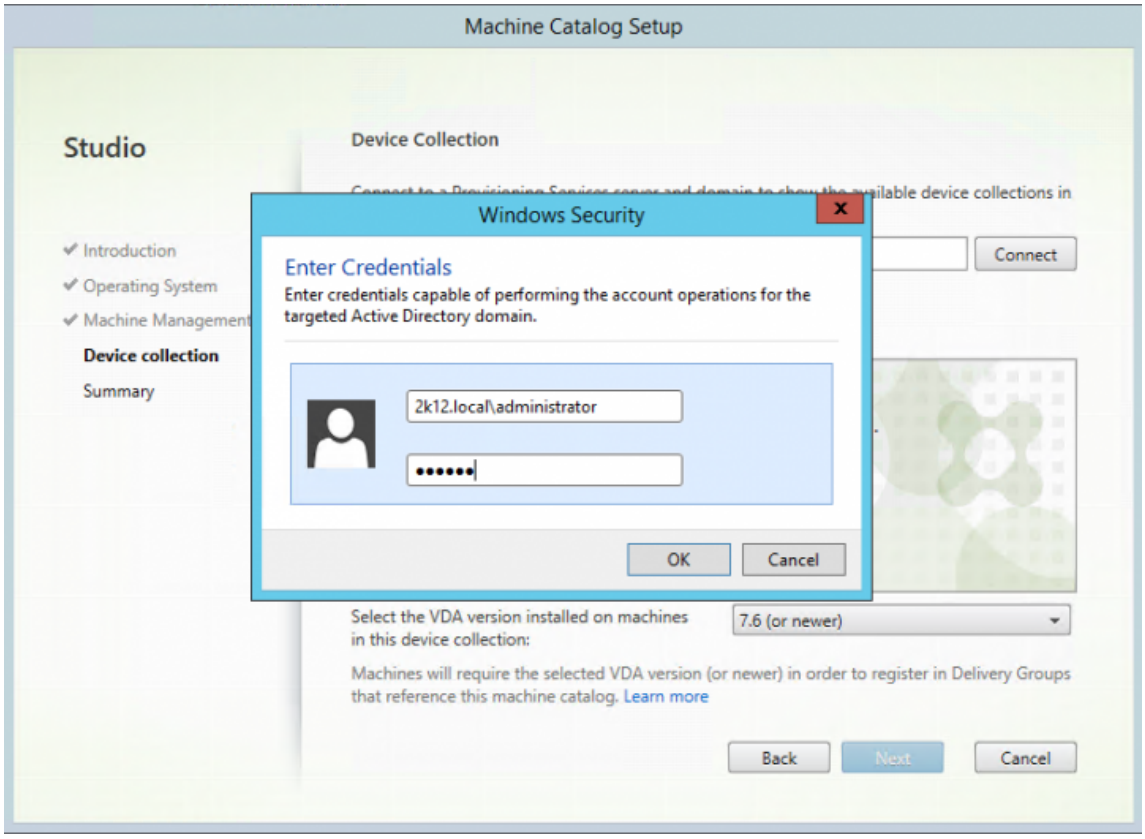
4. Select **Citrix Provisioning**, and click **Next**.



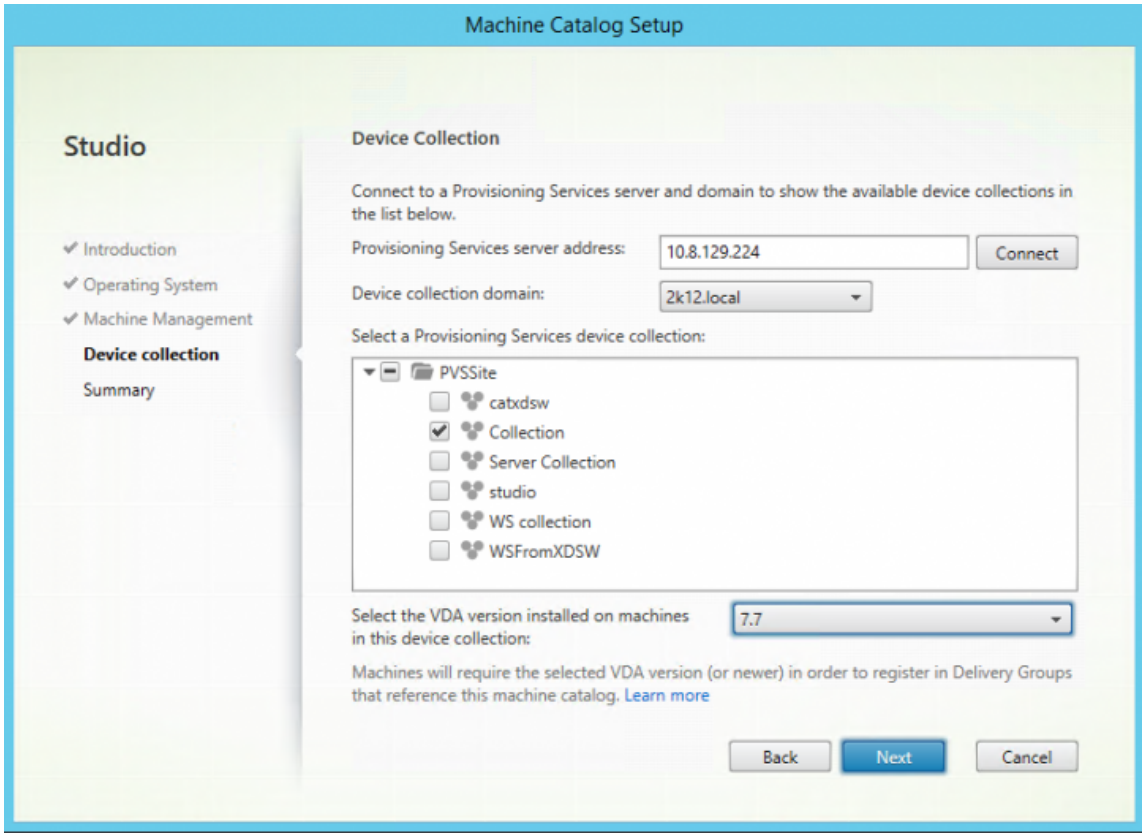
5. On the Device Collection page, provide the address of the Provisioning Server and click **Connect**.



6. Provide the login credentials for the Citrix Provisioning administrator and click **OK**.



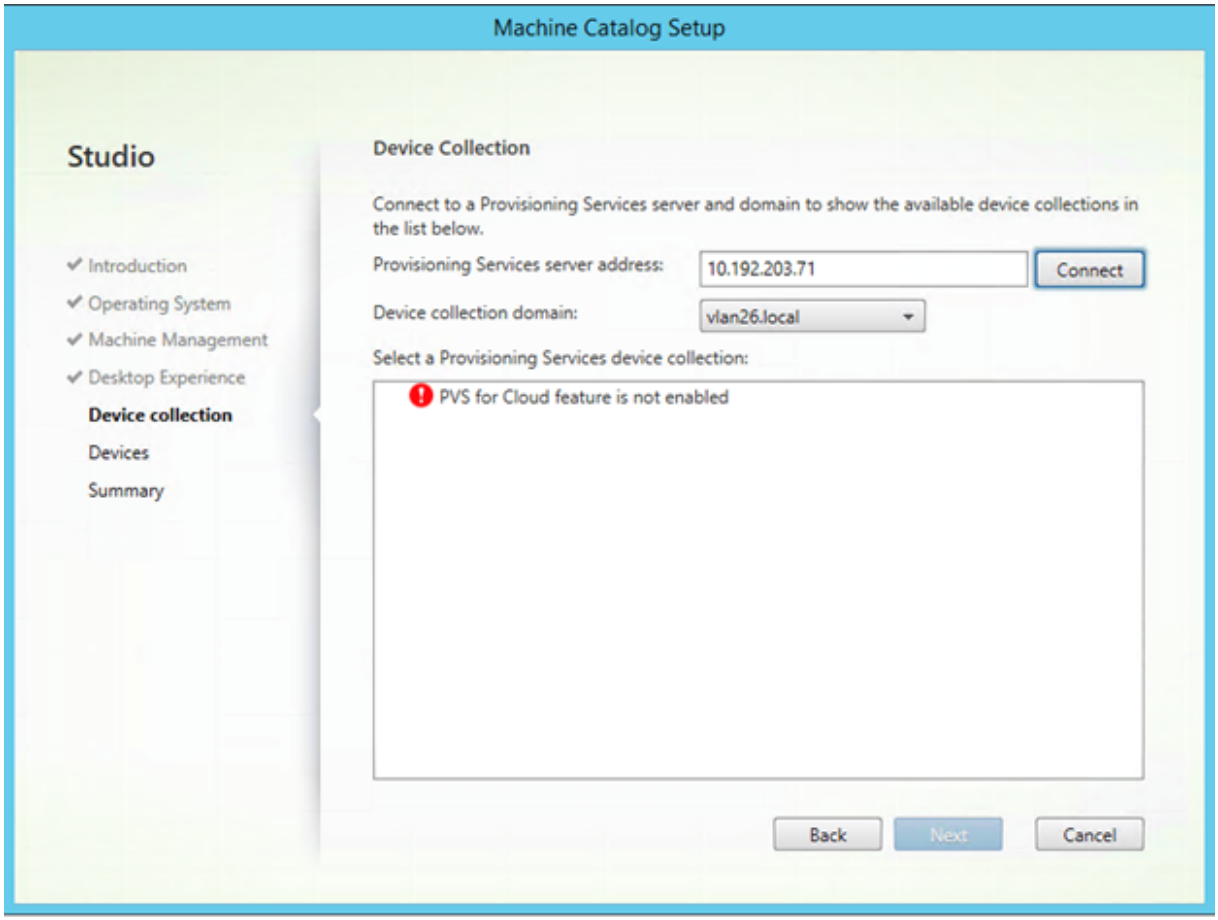
After entering the login credentials, Studio communicates with the Cloud Connector, which then forwards requests to the Provisioning Server using the specified credentials. If a valid Citrix Provisioning administrator is provided, device collections are displayed.



This authentication method represents the only difference between an on-premises Citrix Virtual Apps and Desktops deployment and a Citrix Virtual Apps and Desktops deployment in Citrix Cloud. In an on-premises case, the identity of the Studio user authenticates to the Provisioning Server. In the service model, an explicit authentication is required because Studio runs in an AD environment with no trust relationships to the AD of the Citrix Provisioning deployment.

Error messages in Studio

When setting up a machine catalog using the wizard, the **Device Collection** screen displays the state of Citrix Provisioning cloud connection. If the feature has not been enabled, an error message appears, indicating that “Citrix Provisioning for Cloud feature is not enabled.”



Troubleshooting the Citrix Provisioning Cloud Connector

Use the information in this section to troubleshoot issues related to using the Citrix Virtual Apps and Desktops Setup Wizard for Delivery Controller connectivity.

To verify connectivity

1. Ensure that the Remote PowerShell SDK is installed and properly configured. Verify that the Remote Powershell SDK is installed by executing the following command: CitrixPoshSdk.exe PVS=YES.
2. Uninstall the 5 Citrix Virtual Apps and Desktops snap-ins from the Citrix Provisioning Server and Console.
3. Ensure that the Cloud Connector is on the same VLAN\VNET as the Provisioning Console system, otherwise communication fails.
4. Ensure that the Citrix Provisioning account is also a member of the local Citrix Provisioning OS Admin group.

> **Tip:**
>
> To install the remote PowerShell SDK on the Provisioning Server, you must uninstall the 5 Citrix Virtual Apps and Desktops snap-ins, then install the remote PowerShell SDK.

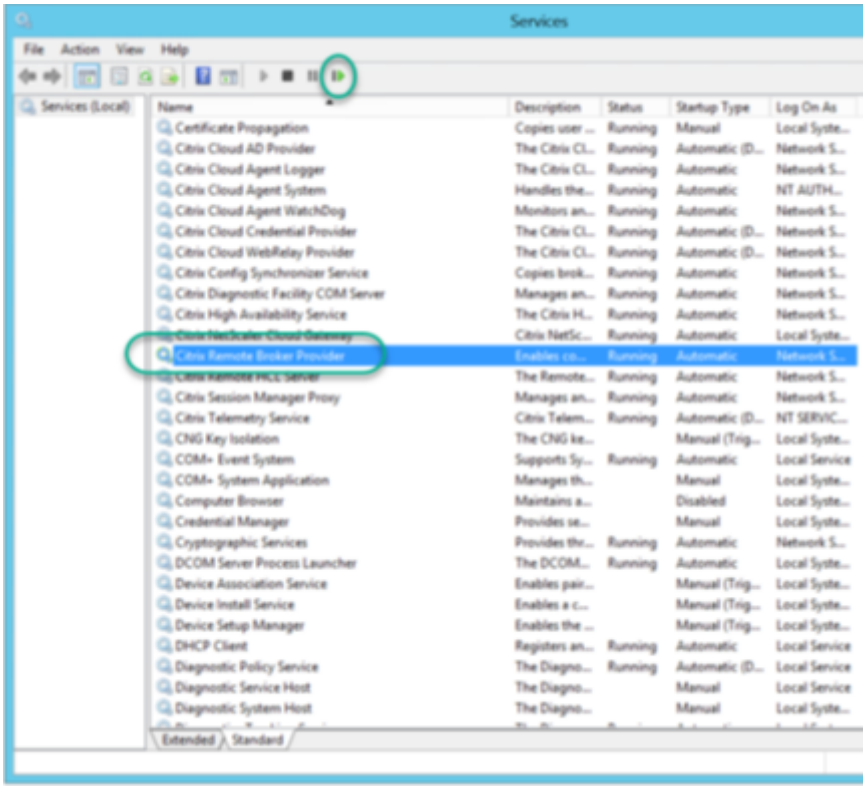
Connection problems between the Provisioning Server and the Delivery Controller

Use the information in this section to troubleshoot connectivity problems between the Delivery Controller and the Provisioning Server.

To verify connectivity:

1. Ensure that the Cloud Connector in the resource location is installed successfully.
2. Ensure that the Cloud Connector is on the same VLAN\VNET as the Provisioning Console system.
3. In Citrix Studio, ensure that the **Zones** screen properly displays the Cloud Connectors.
4. Verify that at least one Cloud Connector is "Connected:"

   a. Sign in to `https://citrix.cloud.com`.
   b. **Under Resource locations > Your Resource Location > Cloud Connectors**, verify that at least one Cloud Connector is showing status as Green.
5. Verify that Citrix Provisioning Support in Citrix Cloud is enabled. Ensure that the **PvsSupport** feature toggle is enabled in the customer's configuration and by the Citrix Cloud administrator.
6. Verify that the Citrix Remote Broker Provider is up and running in the Cloud Connector. Refer to the Cloud Connector to see if the Citrix Remote Broker Provider Service is running.



Considerations when using the Machine Creation Service (MCS) Wizard

Use the information in this section when using the MCS wizard in Studio to import Citrix Provisioning devices into Citrix Virtual Apps and Desktop devices. Verify that:

- Citrix Provisioning devices exist in the collection.
- All target devices are joined to the domain at the same OU.
- A host record of the hypervisor environment where on-prem VMs are located is created in Citrix Virtual Apps and Desktops.
- The correct domain is chosen before the client's domain. This process must occur before connecting to the Provisioning Server in the wizard.

Manage

August 15, 2018

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 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 vDisk 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 vDisk on the network.
- vDisks are streamed to target devices by the Provisioning Server.
- Views used to manage a group of target devices.

Farms

July 2, 2018

A farm represents the top level of a Provisioning Services infrastructure. Farms provide a "Farm Administrator" with a method of representing, defining, and managing logical groups of Provisioning Services 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 Console, those objects display in the tree.

The wizard also prompts you for additional farm information such as the name of the license server, your user account information, and those servers that can serve the bootstrap file to target devices. You can always rerun the wizard to change settings. You can also 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 Provisioning Services Console in the Console tree, then select **Connect to farm**.
2. Under **Server Information**, 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 the Windows credentials that you are currently logged with, then optionally enable the Auto-login on application start or reconnect feature.
    - Use different Windows credentials by entering the username, password, and domain associated with those credentials, then optionally enable the Save password and Auto-login on application start or reconnect feature.

4. Click **Connect**. The Farm icon appears in the Console tree.

Managing Connections

You can manage connections to farms from the **Manage Connections** dialog box. To open the dialog, right-click on the Provisioning Services Console icon in the tree, then select the **Manage Connections** menu option.

Sites

July 2, 2018

A site provides a method of representing and managing logical groupings of 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 document: Managing Stores

Some site-level tasks include:

- Defining Device administrator and device operator roles.
- Managing Provisioning Servers
- Managing connections
- Creating a New Site in a Farm, as described in this document: Rebalancing Devices on the Provisioning Server
- Importing Target Devices into Collections
- Accessing auditing information

To create a new 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 will have the site administrator rights in this site. The Add Security Group dialog appears.
4. Check the box next to each group, then click OK. Optionally, check the Domains/group Name checkbox 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 should reside (this feature must first be enabled in the farm's properties).

To modify an existing site's properties, right-click on the site in the Console, then select Properties. Make any necessary 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 button:** Type the name of this site in the textbox.
- **Description:** Optional. Type the description of this site in the textbox.

Security Tab:

- **Add button:** Click the Add button to open the Add Security Groups dialog. Check the box next to each group to which site administrator privileges should apply. To add all groups that are listed, check the Domain\Group Name check box.
- **Remove button:** Click the Remove button to remove site administrator privileges to select 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 will 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 and the MAK tab appears to allow credential information to be entered. After the credentials are entered, click OK and the Manage MAK Activations dialog re-appears.

Options Tab:

- **Auto-Add:** Select the collection that the new target device will be added to from the drop-down menu. (This feature must first be enabled in the farm properties.) Set the number of seconds to wait before Provisioning Services scans for new devices on the Seconds between inventory scans scroll box. Default is 60 seconds.

vDisk Update Tab:

- **Enable automatic vDisk updates on this site:** Select this check box to enable automatic vDisks to occur, then select the server that should run the updates for this site.

Servers

July 2, 2018

A Provisioning Server is any server that has Stream Services installed. Provisioning 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, Provisioning Servers get the vDisk from a shared-storage device on the network.

Provisioning Servers also retrieve and provide configuration information to and from the Provisioning Services database. Provisioning Server 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 re-run on a Provisioning Server at a later date in order to change network configuration settings).

After the Provisioning Server software components are successfully installed, and the wizard configurations have been made, servers are managed through the Provisioning Services Console.

> **Tip:**
>
> When configuring PVS servers, ensure proper firewall isolation is observed so that the deployment provides a robust security boundary around all servers, including the SQL server and disk storage, so that network access outside the security boundary is restricted to prevent viewing of weakly authenticated or unencrypted data flows.
>
> At a minimum, isolate only those PVS server instances that communicate with one another on their unauthenticated intra PVS server communication channels. To achieve this, 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. This should prevent unauthorized users from targeting these additional components.

Provisioning servers in the console

A Provisioning Server is any server that has Stream Services installed. Provisioning 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, Provisioning Servers get the vDisk from a shared-storage device on the network.

Provisioning Servers also retrieve and provide configuration information to and from the Provisioning Services database. Provisioning Server 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 re-run on a Provisioning Server at a later date in order to change network configuration settings).

After the Provisioning Server software components are successfully installed, and the wizard configurations have been made, servers are managed through the Provisioning Services Console. The Console is used to perform Provisioning Server management tasks such as editing the configuration settings or the properties of existing Provisioning Servers.

Provisioning Servers appear in the Console main window as members of a site within a farm. To manage Provisioning Servers that belong to a specific site, you must have the appropriate administrative role (Site Administrator for this site, or Farm Administrator).

> **Note:**
>
> In the Console, the appearance of the Provisioning Server icon indicates that server's current status.

In the Console, Provisioning Servers are managed by performing actions on them. The following actions can be performed. To view a list of actions that can be performed on a selected Provisioning 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 (refer to "Management Tasks" for task details).

Showing Provisioning Server connections

To view and manage all target device connections to the Provisioning Server:

1. Highlight a Provisioning Server in the Console, then select Show connected devices from the Action menu, right-click menu, or Action pane. The Connected Target Devices dialog appears.
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.

Option	Description
Message	Opens the Edit Message dialog to allow you to type, and then send a message to target device(s) highlighted in the dialog.

Note: When selecting Shutdown or Reboot, a dialog opens providing the option to type a message that displays on the effected devices. The Shutdown or Reboot options can be delayed by entering a delay time setting.

If a message appears confirming that the target device was successfully shut down or rebooted, but the icon in the Console window does not change accordingly, 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 vDisk.

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 vDisk, the following additional load balancing algorithm customizations can be set:
    - Subnet Affinity – When assigning the server and NIC combination to use to provide this vDisk to target devices, select from the following subnet settings:
        - None – ignore subnets; uses least busy server. This 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 vDisk.
    - Rebalance Enabled using Trigger Percent – Enable to rebalance the number of target devices on each server in the event that the trigger percent is exceeded. When enabled, Provisioning Services checks the trigger percent on each server approximately every ten minutes. For example: If the trigger percent on this vDisk is set to 25%, rebalancing occurs within ten minutes if this server has 25% more load in comparison to other servers that can provide this vDisk.

> **Note:**
>
> The load balance algorithm takes into account the Server Power setting of each server when determining load.

Load balancing will not occur 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 (preventing load shift thrashing during a 'boot storm').

Load balancing is also considered when target devices boot. Provisioning Services determines which qualified Provisioning Server, with the least amount of load, should provide the vDisk. Whenever additional qualified servers are brought online, rebalancing will occur automatically.

To implement load balancing in a HA network configuration

- Assign a power rating to each Provisioning Server on the Server Properties' General tab.
- For each vDisk, 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 are not using a vDisk that is in HA mode will not be diverted to a different server. If a vDisk is misconfigured to have HA enabled, but they are not using a valid HA configuration (Provisioning Servers and Store , target devices that use that vDisk can lock up.

To rebalance Provisioning Server connections manually

1. In the 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 vDisk access updates

To check for updates to vDisks that the selected Provisioning Server has access to:

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 vDisk is automatically updated or is scheduled to be updated.

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 will be 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 checkbox.
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 re-run the Configuration Wizard to re-start 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

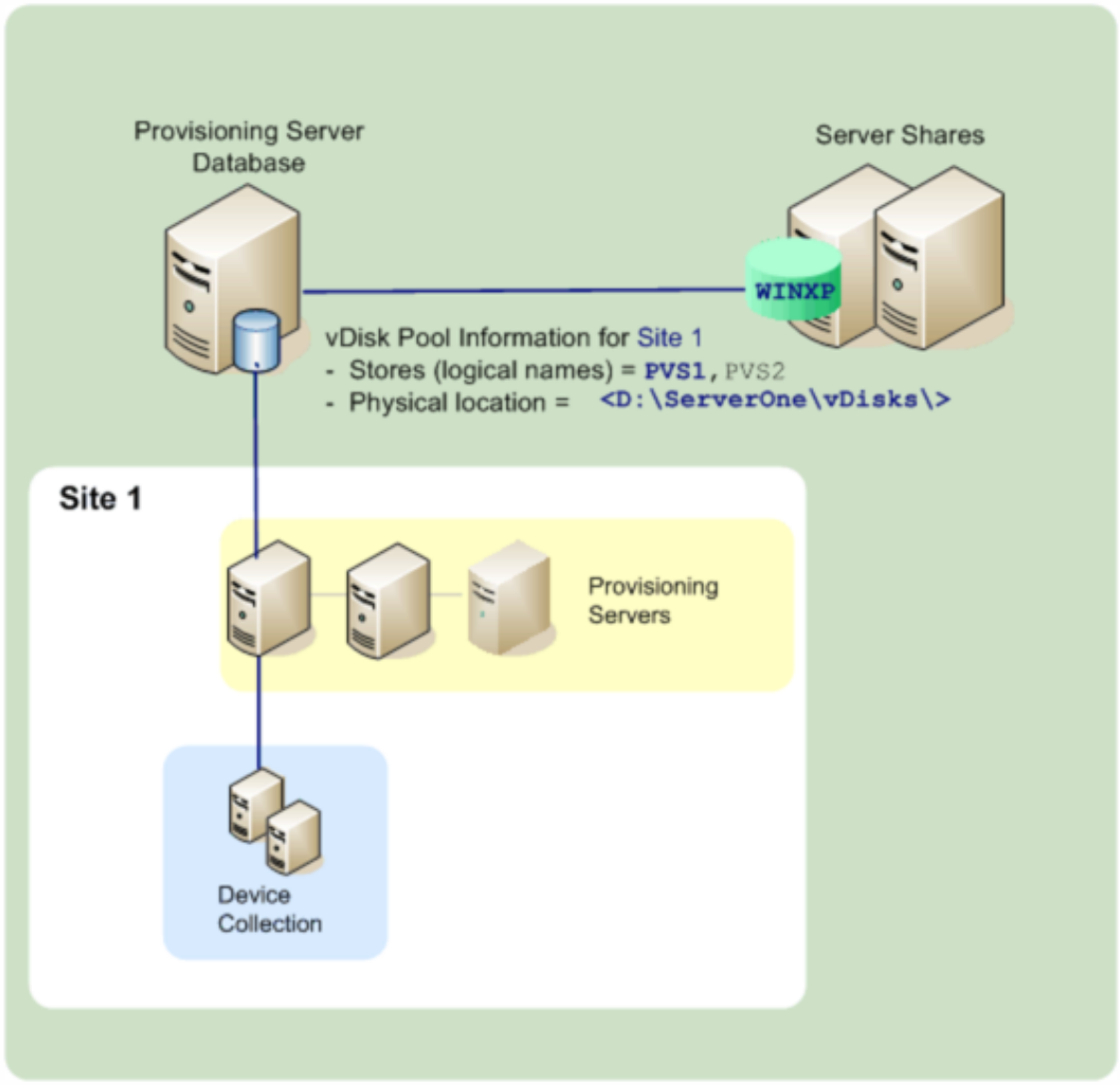
For each store, select the Provisioning Servers that can access that store:

1. In the 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 that should be able to access this store exists.
3. Enable the checkbox next to each Provisioning Server that can provide vDisks in this store, then click OK.

Stores

August 29, 2018

A store is the logical name for the physical location of the vDisk folder. This folder can exist on a local server or on shared storage. When vDisks files are created in the Console, they are assigned to a store. Within a site, one or more Provisioning Servers are given permission to access that store in order to serve vDisks to target devices.



A Provisioning Server checks the database for the Store name and the physical location where the vDisk resides, in order to provide it to the target device

Separating the physical paths to a vDisks storage locations 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 vDisk from another Provisioning Server that has access to the store and permissions to serve the vDisk.

If necessary, copies of vDisks can be maintained on a secondary shared-storage location in the event

that connection to the primary shared-storage location is lost. In this case, the default path can be 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 (the default path is not valid for that server, not because of a connection loss, but because it is simply not valid) then an override path can be set in the store properties for that particular server. Provisioning Servers will always use either the default path (if the override path does not exist in the database) or the override path if it does exists 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 may 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 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 (logical name for this storage location) and a description of this store.
3. Optionally, select the site that will act as 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 this procedure is performed by a site administrator, only those sites that they administer appear.)
6. On the Paths dialog, type or browse for the default path for this store (physical location of the vDisk folder). Optionally, a new folder can be created by clicking on the browse button, and then clicking on Create New Folder. If the user is a site administrator, only those sites that they administer will be available in the list.
7. The write cache path(s) for the selected store display under the paths list. Optionally, a new store cache folder can be created by clicking on the browse button, and then clicking on Create

New Folder. Additional write cache paths can be added for use by the store by clicking Add. Entering more than one write cache paths allows for vDisk load to be distributed to physically different drives. When a target device first connects, the Stream Service picks from the list. If using HA, 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 here.

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 this store will use, 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

A store can be created when the Configuration Wizard is run or in the Store Properties dialog. The store properties dialogs allows you to:

- Name and provide a description of the store.
- Select the owner of the store (the site which will manage the store).
- Provide a default path to the store (physical path to the vDisk).
- 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 Provisioning Services database. Each site has one vDisk Pool, which is a collection of vDisk information required by Provisioning Servers that provide vDisks in that site. The vDisk information can be added to the vDisk 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, PVS-1
  - View or type a description of this store.
- **Description:** View or type a description of this store.
- **Site that acts as owner of this store:** Optional. View or scroll to select the site that will act 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 vDisk 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 setting an override store path on the Server's Properties dialog, the path must be set prior to creating a new version of the vDisk. Because this path information is stored and referenced in the .vhdx header information, changing the path after versioning may 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 vDisk 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

July 2, 2018

Device collections provide the ability 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 could represent a physical location, a subnet range, or a logical grouping of target devices. For example, a collection could consist of all target devices that use a particular vDisk image, and that target device collection might consist of maintenance, test, and production devices. Alternatively, three device collections could exist for a particular vDisk; one consisting of production devices, one consisting of test machines, and another consisting of maintenance machines. In the proceeding examples, all of the devices in a given collection are assigned to the same vDisk.

Depending on a sites preference, another collection use case might include the consolidation of test and/or maintenance devices into a single device collection, and then managing vDisk 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 vDisk.

Device collections are created and managed by farm administrators, or site administrators that have security privileges to that site, or device administrators that have security privileges to that collection.

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 allowing you to view or make modifications to that collection.

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 target device information from a file. The target device information must first be saved as a.csvfile, it can then be imported into a device collection.

> **Note:**
>
> The.csvtext file can be created with a.txtfile,NotePad.exe or Excel. It contains one line per target device, which is formatted as follows:
>
> 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

The wizard can be accessed from the farm, site, and device collection right-click menus. If accessed from the site or collection, only those target devices in the import file that match the site and collection by name, will be 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 already 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. The file is located in:

C:\Documents and Settings\All Users\Application Data\Citrix\Provisioning Services\log

To Import target devices into a Collection

1. In the Console, right-click on the device collection that the target devices should be imported to, 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 below. 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 checkbox.
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 Console

After making changes to a collection, it may be necessary to 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 tree, then select the Target Device>Boot menu option. The Target Device Control dialog displays with the Boot devices menu option selected in the Settings drop-down 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 drop-down 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 tree, 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 drop-down 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 shutdown 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 drop-down 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 drop-down menu, select the collection to move this target device into, then click OK to close the dialog.

Target devices

July 2, 2018

A device, such as desktop computer or server, that boots and gets software from a vDisk on the network, is considered a target device. A device that is used to create the vDisk image is a considered a Master Target device.

The lifecycle of a target device includes:

- Preparing
  - A Master target device used for creating a vDisk image
  - A target device that will boot from a vDisk 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, the device itself must be configured to allow it to boot from the network, a vDisk must be assigned to the device, and a bootstrap file must be configured to provide the information necessary for that device to boot from the assigned vDisk.

There are several types of target devices within a farm. For example, while a device is being used to create a vDisk 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 vDisk 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 vDisk that is currently in production (default).

- Maintenance: Select this option to use this target device as a Maintenance device. Only a Maintenance device can access and make changes to a vDisk version that is 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 Provisioning Services database. Target Device properties include information such as the device name and description, boot method, and vDisk assignments (refer to Target Device properties for details).

Target Devices are managed and monitored using the Console and Virtual Disk Status Tray utilities.

In the 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

> **Note:**
>
> 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.

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, unless that name is the same as the machine name being imaged. When the target device boots from the vDisk, the name entered here becomes the target device machine name.
Description	Provides a description to associate with this target device.

Field	Description
Type	Select the access type for this target device from the drop-down list, which includes the following options: **Maintenance** - Select this option to use this target device as a Maintenance device which will to apply updates to a new maintenance version of a vDisk. 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 vDisk in order to facilitate QA testing of a vDisk version in Standard Image mode, prior to the release of that version to production machines. **Production** - Select this option to allow the target device to stream an assigned vDisk that is currently in production. Production devices have shared, read-only access to production versions of a vDisk. Production devices do not have access to maintenance or test versions, which prevents updates that have not been tested 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 this target device should use. Options include booting from a vDisk, hard disk, or floppy disk.
MAC	Enter the media access control (MAC) address of the network interface card 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 the same port), you must change this value.

Field	Description
Class	Class used for matching new vDisks to target devices when using Automatic Disk Image Update in order 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.

vDisk tab

Field	Description
vDisks for this device	Displays the list of vDisk assigned to this target device, including the following options: Click **Add** to open the Assign vDisks dialog. To filter the vDisks that display, select a specific store name and Provisioning Server or select All Stores and All Servers to list 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 vdisk is listed in the table or if either (or both) secondary boot options are enabled, the user is prompted with a disk menu at the target devices 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 from those available to this target device.
Name and string	There is 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 "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**.

Authentication tab

Password information entered in this dialog is for initial target device login only. It does not affect Windows account login.

Field	Description
Authentication	If authenticating with a user name and password, enter the user name for the account. Follow your organization's user name conventions. **Note:** User names must be at least two characters and no more than 40 characters in length. User names are NOT case sensitive. Authentication methods include: None, Username and password, External verification (user supplied method)
Username	If the account already exists, you cannot change the user name.
Password	If authenticating with a user name and password: Click the **Change** button to open the Change Password dialog. To create a new password for a user account, type the old password, then type the new password in both the New password and Confirm new password text boxes. Click OK to change the password. **Note:** Follow your organization's password conventions. Requires passwords be at least three characters and no more than 20 characters in length. Passwords ARE case sensitive. Re-enter the new password exactly as you entered it in the previous field to confirm it.

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, XenApp License, or XenDesktop License).

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 could 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 that use personal vDisks are created and added to a collection when the XenDesktop Setup Wizard is run. If a target device template exists, it is ignored when the target device that uses a personal vDisk 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 Set device as template.

Consider the following when using templates:

- Disable the target device that serves as the template to permit all target devices using this template to be added to the database, but 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 will be taken from the default template target device. No user interaction is required.

Creating a VM with nested virtualization

In some cases, you may 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 Device Guard, PVS has no means to know if this functionality was setup for that particular VM. To resolve this issue, you can manually enable Device Guard on the Hyper-V host using a PowerShell command after the VM has been created using the XenDesktop Setup Wizard.

To configure a VM to use Device Guard:

1. Create the VM using the XenDesktop Setup Wizard.
2. After creating the VM, execute 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:**
>
> Refer to 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 personal vDisks can only inherit the properties of another target device that uses a personal vDisk.

1. In the 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 checkbox 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 will 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 drop-down 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 currently 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:
    - Current status (active or inactive)
    - IP address
    - Current Provisioning Server
    - Current vDisk name
    - Provisioning Server cache file size in bytes

      Also, in the Console window, if the target device is active, 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 should 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 drop-down menu. Target devices are 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 target devices successfully receives the message, the status changes to Success.

Shutting down target devices

To shutdown target devices:

1. Right-click on the collection to shut down all target devices within the collection, or highlight only those target devices that should be 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 drop-down 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 shutdown 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 that should be restarted within the collection, then select the Restart devices menu option. The Target Device Control dialog displays with the Restart devices menu option selected in the Settings drop-down 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 using drag and drop in the Console's details pane (drag the device(s) 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 drop-down menu, select the collection to move this target device into. If applicable, apply the collection's device template to the target device being moved, by enabling Apply target collection's template device properties to moved devices.
3. Click Move.

> **Tip:**
>
> There is a risk that moving target devices from site to site could cause them to be deleted in the future. This risk increases if the target device was created using the Streamed VM Setup Wizard. While an administrator can use the interface to move target devices from site to site, Citrix recommends that you avoid moving them from site to site in this fashion.

Managing target device Personality

Normally, all target device's sharing the same vDisk 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 can then be used by your custom applications and scripts for a variety of purposes.

For example, suppose you are using Provisioning Server to support PCs in three classrooms. Each classroom has its own printer, and you want the PCs in each classroom to default to the correct printer. By using the Target Device Personality feature, you can define a default printer field, and then enter a printer name value for each target device. You define the field and values under Target Device Properties. This information is stored in the database. When the target device boots, the device-specific printer information is retrieved from the database and written to an .INI file on the vDisk. Using a custom script or application that you develop, you can retrieve the printer value and write it to the registry. Using this method, each time a target device boots, it will be set to use the correct default printer in its classroom.

The number of fields and amount of data that you can define for each target device is limited to 64Kb or 65536 bytes per target device. Each individual field may be up to 2047 bytes.

Target Device Personality Tasks

- Define personality data for a single target device using the Console
- Define personality data for multiple target device 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 limits to the total amount of personality data assigned to a single string (names and data combined) is approximately 2047 bytes. Also, the total amount of data contained in names, strings and delimiters is limited to approximately 64Kb or 65536 bytes per target device. This limit is checked by the administrator 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. This data will be inherited

when new target devices are added automatically to the database by either the Add New Target Device Silently option, or with the Add New Target Device with BIOS Prompts option.

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 additional 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 device 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 to, then right-click and select the Paste device properties menu.
3. Click on the Personality strings option (you may also choose to copy other properties at this time), then 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 vDisk file system for easy access by your custom scripts or applications.

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. It can be queried by the standard Windows .INI API. Additionally, a command line application, called GetPersonality.exe, is provided to allow easier batch file access to the personality settings.

A target device's vDisk name and mode can be retrieved using GetPersonality.exe. The following reserve values are included in the [StringData] section of the Personality.ini file:

```
$DiskName=<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 is the name of the disk. A vDisk 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
```

Examples:

Setting a Registry Key Value:

The example below retrieves the Target Device Personality data value from the DefaultPrinter field and writes it to the target device registry to set the default printer for the device.

The Target Device Personality String Set in Target Device Properties is:

```
DefaultPrinter= \CHESBAY01\SAVIN 9935DPE/2035DPE PCL 5e,winspool,
   Ne03:
```

A batch file run on the target device would include the following line:

```
GetPersonality DefaultPrinter /r=HKEY_CURRENT_USER\Software\
   Microsoft\Windows NT\CurrentVersion\Device
```


> **Note:**
>
> The actual key name should be the UNC name of the network printer, such as \dc1\Main, and the value that should be entered for the key would be similar to winspool,Ne01: where Ne01 is a unique number for each installed printer.

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 would then need to be included in the batch file:

```
GetPersonality Pathname /f=temp.txt
set /p Path= <temp.txt
```

   > **Note:**
   >
   > If the filename specified with the /f option already exists, GetPersonality will not append the line to the file. Instead, the existing line is overwritten in the file.

Changing the device status to Down

Occassionally, a target device may display as active when it is actually down. This 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 steps that follow.

1. In the Console, right-click on the target device that should be marked as down, then select the Mark Device Down option. A confirmation dialog appears.
2. Click OK to mark the device as down.

vDisks

September 21, 2018

vDisks are managed throughout the vDisk lifecycle. Full image lifecycle takes a vDisk from initial 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

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. Citrix Provisioning also provides the option to create a common image for use with a single target platform or for use with multiple target platforms. For details, refer to 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, refer to *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, refer to 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, refer to Retiring a vDisk.

> **Note:**
>
> In addition to those vDisk tasks performed within a vDisk'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, refer to Configuring a vDisk for Microsoft Volume Licensing.
- Enabling Active Directory machine account password management, if applicable.
- Enabling printer management (for details, refer to Managing Printers.
- More settings:
  - Enabling or disabling the streaming of this vDisk to assigned target devices. For details, refer to vDisk Properties dialog.
  - Providing vDisk identification information. For details, refer to Identification information in the vDisk Properties dialog.

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 server side persistent write cache. Persistent cache should only be used where unauthorized users have unprivileged 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 2007 - all	Not supported	Not supported	Not supported
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 2007 - all	Not supported	Not supported	Not supported
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:**
>
> Citrix Provisioning 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, refer to 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, refer to 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 select the correct bootstrap from the Console, right-click on the Provisioning Server, select Configure Bootstrap. On the General tab, click on the drop-down **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, refer to 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 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 should be reconsidered to accommodate the streaming workload. To ensure target device reliability in 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 IO 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 vDisk IOs 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 IO and network traffic.

For extra security, the Provisioning 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 should be manually deleted.

Invalidating changes include:

- Placing a vDisk in Maintenance
- vDisk is placed in Private Image mode
- Mapping the drive from the Console
- Changing the location of the write cache file
- Using Automatic update

> **Tip:**
>
> Consider the impact of using server side persistent write cache. Persistent cache should only be used where unauthorized users have unprivileged access to a machine. Ensure that machines are not shared among users.

Selecting the write cache destination for standard vDisk images

August 22, 2018

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 server side persistent write cache. Persistent cache should only be used where unauthorized users have unprivileged access to a machine. Ensure that machines are not shared among users.
- If you are 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 using cache on the target device RAM and Standard Image mode, the max size of the RAM write cache is determined by the registry setting **WcMaxRamCacheMB** in the BNIStack Parameters. This registry setting is a DWORD parameter. If the registry entry does not exist, then the default value used is 3584 MB.
- Support for the Microsoft System Center Configuration Manager (ConfigMgr) Client is as follows:

ConfigMgr Client	Cache on device hard drive	Cache in device RAM with overflow on hard disk	Cache in device RAM
ConfigMgr 2007 - all	not supported	not supported	not supported

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 2007 - all	not supported	not supported	not supported
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:**
>
> Citrix Provisioning version 7.12 introduced Linux streaming. When using this feature, consider that caching options on a Linux target device are the same as on a Windows device. For more information about Linux streaming, refer to the installation article.

Cache on device hard drive

Write cache can exist as a file in NTFS format on the target-device's hard drive. This write cache option frees up the Provisioning Server since it does not have to process write requests and 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, refer to 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 select the correct bootstrap from the Console, right-click on the Provisioning Server, select Configure Bootstrap. On the General tab, click on the drop-down 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, refer to the Deprecation article.

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.

> **Tip**
>
> 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. The local disk free space should be reconsidered to accommodate the streaming workload. To ensure target device reliability in 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 IO 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. Thus, 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 IOs 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 IO and network traffic.

For extra security, the Provisioning 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.

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 should be manually deleted.

Invalidating changes include:

- Placing a vDisk in Maintenance
- vDisk is placed in Private Image mode
- Mapping the drive from the Console
- Changing the location of the write cache file
- Using Automatic update

> **Tip:**
>
> Consider the impact of using server side persistent write cache. When administering this functionality, persistent cache should only be used where unauthorized users have unprivileged access to a machine. Ensure that machines are not shared among users.

Support for replicated vDisk storage

August 3, 2018

Citrix Provisioning supports the replication of vDisks on stores that are local (local/attached storage on Provisioning Servers) within a site.

Replication considerations include:

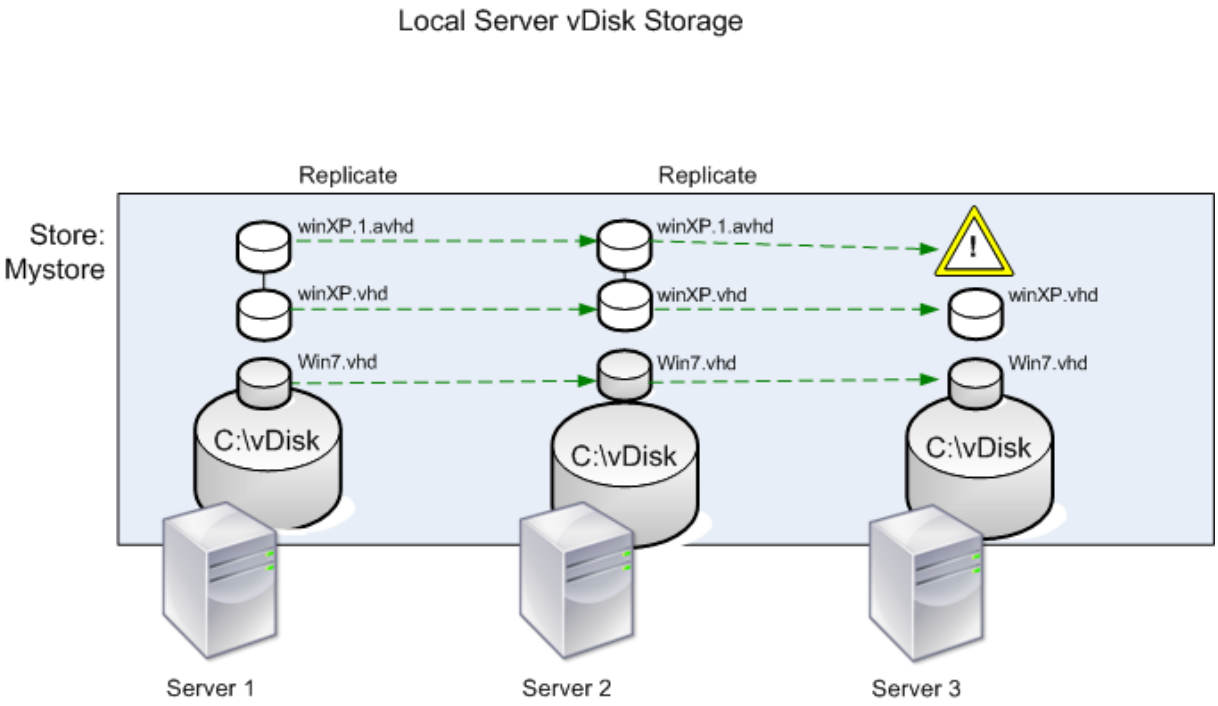
- All Provisioning Servers must have network connectivity with all other servers in the farm.
- Replication must be properly configured to work with Citrix Provisioning and meet all requirements.
- Replicated files include: *.vhdx, *.avhdx, and *.pvp. If you are importing existing vDisks, the *.xml (manifest files) may also be replicated. The *.lok files should not be 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 prior to creating a new version of the vDisk. Because this path information is stored and referenced in the .vhdx header information, changing the path after versioning may 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 follwing 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 Console, then select the Versions menu option. The vDisk Versions dialog appears.
2. Highlight a version in the dialog, then click the Replication button. 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 a 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 columns 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 a orange warnings under that version column.

Exporting and importing vDisks

August 15, 2018

Citrix Provisioning exports and imports both *versioned* and *unversioned* vDisks from an existing store to another store in a different farm.

> **Tip:**
>
> If you are importing VHDs that are not exported using Citrix Provisioning, all differencing disks must first be merged to a base disk using third party tools. After merging them, import the new VHD base disk.

Exporting vDisks

To export a vDisk

1. Right-click on the vDisk in the Console, then select the **Export** menu option. The Export dialog appears.
2. Select the version to export from the drop-down 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. Af-

> ter 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.

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 tree pane, 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** drop-down menu.
4. Select the server to use to search for vDisks from the **Server to use for searching** drop-down menu, then click **Search**. All vDisks in the store display in the **Add checked vDisks to the vDisk Pool**.
5. Check the vDisks that should be 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 tree pane, 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** drop-down menu.
4. Select the server to use to search for vDisks from the **Server to use for searching** drop-down menu, then click **Search**. All vDisks in the store display in the **Add checked vDisks new versions**.
5. Check those vDisk versions that should be added to the vDisk pool.
6. Click **Add** to add the vDisk(s) to the vDisk pool.

Releasing vDisk locks

August 8, 2018

Since multiple target devices and Provisioning Servers can gain access to a single vDisk image file, it is necessary to control access to prevent corruption of the image. Should a user accidentally assign a private image to multiple target devices, and then try to boot those target devices, a corrupt image would result. Therefore, the image becomes locked appropriately for a given configuration. The locked vDisk icon appears with a small 'lock' on it.

Be aware that under certain circumstances these locks may not be released properly. A lock on a vDisk image may not be released properly when a target device machine is booted from a vDisk, and then fails (or power is lost). 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 will not be able to mount that vDisk because a lock is still held by the failed target device. The Administrator has the capability to 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, may corrupt the image.

To release select vDisk locks

1. In the 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 device 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

August 3, 2018

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 Console, right-click on the vDisk that has the properties settings that you want to share with other vDisks, then 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

August 15, 2018

If vDisks exist in a store, and used by target devices in your site, you can add them to the site's vDisk Pool. In the 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 drop-down menu. If you accessed this dialog from the store, select the site where vDisks are added using the drop-down menu.
4. In the **Select the server to use when searching for new vDisks** drop-down menu, select the Provisioning Server that performs the search. Click Search. Any new vDisks that do not exist in the database display in the text box below.
5. Check the box next to each vDisk that you want to add, or click Select All to add all vDisks in the list, then click **Add**.

Backing up a vDisk

August 3, 2018

The 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, to restore it requires simply replacing the corrupted file with a previous, functional version.

Do not back up a vDisk while it is in use or while it is locked. It is recommended to integrate the backing up of vDisks into your normal Provisioning Server backup routine.

Viewing vDisk usage

August 3, 2018

To view target devices that are connected to a specific vDisk

1. Right-click a vDisk in the 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 currently being served by a Provisioning Server

1. Right-click on a 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

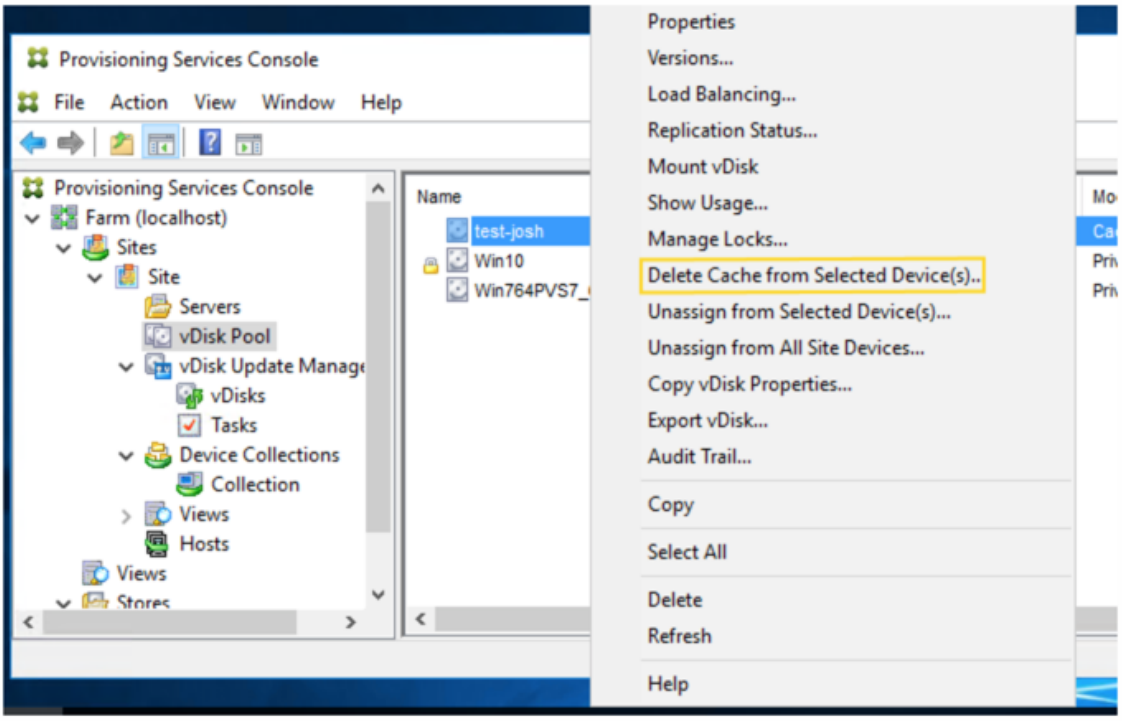
August 3, 2018

The Delete Cache from Selected Device(s) context menu option allows you to manually delete cache on a difference disk. The option is only available if the vDisk cache mode is set to **Server Persistent Cache**.

> **Note:**
>
> Write cache on a Difference Disk is not automatically deleted if that file becomes invalid. Files marked as invalid should periodically be deleted manually.

To delete a cache on a Difference Disk

1. In the Console, right-click on the vDisk that is associated with difference disk files you want to delete. Select the **Delete Cache from Selected Device(s)** menu option.



   The Delete Cache for Devices dialog box appears.

2. Check each target device for which the cache should be deleted, 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

August 3, 2018

This article describes how vDisk version access modes relate to target device types, and how to assign and unassign a vDisk 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 as well as their relationship to each other.

A version's access mode is managed on the vDisk **Versioning** dialog. New versions of a vDisk are generally 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 in order 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 because the scheduled release date and time has not been reached and/or the version it is not yet available to all servers in the site. If the Boot production devices from version drop-down list is set to Newest released, after the release date and time is reached and all servers are able to access this version, access changes to Default. If access displays as blank, this version is considered released to production, however it is not the version currently selected as the version from which Production devices should boot.
- **Default** – read-only version that is bootable by all device types. If the Boot production devices from version is set to Newest released, then the latest released production version is marked with a green checkmark and 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 version drop-down list, then that version is marked with a green checkmark and the 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 version drop-down list, then that version is marked with a green checkmark and the 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 drop-down list (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 when the managed vDisk is created.

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 do this, a new version is requested from the vDisk Versions Dialog, which creates a new read/write differencing disk and places that newly created version in **Maintenance Access** mode. While in Maintenance mode, this version of the vDisk can only be accessed by a single maintenance device (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, this version of the vDisk can only be streamed to Test or Maintenance devices to which it is assigned. This allows the new version to be tested before being released into the production environment, and permits Production devices to continue to stream from the previous version without interruption. If issues are found, this version can be reverted back into Maintenance mode.

  If you are testing a device that uses a personal vDisk, use the assigned PvD Test device to test vDisk updates.

- **Production Devices**

  After successfully testing the new version, that version 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 back into either Test or Maintenance mode after any booted devices accessing this version are shut down.

If a device is assigned a personal vDisk, after the updated vDisk is tested using a PvD Test device, you can change the device to be a PvD production device, which allows you to continue testing for compatibility within your production environment.

- **Update Devices**

Update devices are used to update a Managed vDisk. Update Devices are created automatically when the Managed vDisk Setup Wizard is run. Only one Update device exists for each managed vDisk, and that vDisk and Update device are given the same name. For more information on Managed vDisks, refer to vDisk Update Management.

Unassigning vDisks from target devices

> **Note:**
>
> The Unassign from All site Devices option only unassigns vDisks that are not personal vDisks. When a personal vDisk is deleted, the vDisk's Update Device is also deleted.

1. Select the vDisk in the Console, then right-click and select the Unassign from Selected Device(s) 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.

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 drop-down 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 current status of each version:

  - Wrench icon indicates that this version's access mode is set to Maintenance (read/write) mode, from which only a single maintenance device can boot.
  - Magnifying glass icon indicates that this version's access mode is set to Test, from which only a test device can boot.

  - 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.
  - Green checkmark icon indicates that this version is the current production version based on settings selected on the Boot production devices from version drop-down menu. All device types can boot from vDisk version that is in production.
  - 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 to be released 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 has 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, then the latest released production version is marked with a green checkmark and the 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 drop-down list, 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 drop-down list (Production, Maintenance, or Test). The default Farm Properties setting is available on the vDisk Versions tab. A wrench icon is shown for 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 new 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 will be shut down prior to 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 will display 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 on 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 yet.

- Text

  The text box provides a description of the currently selected version.

Updating vDisks

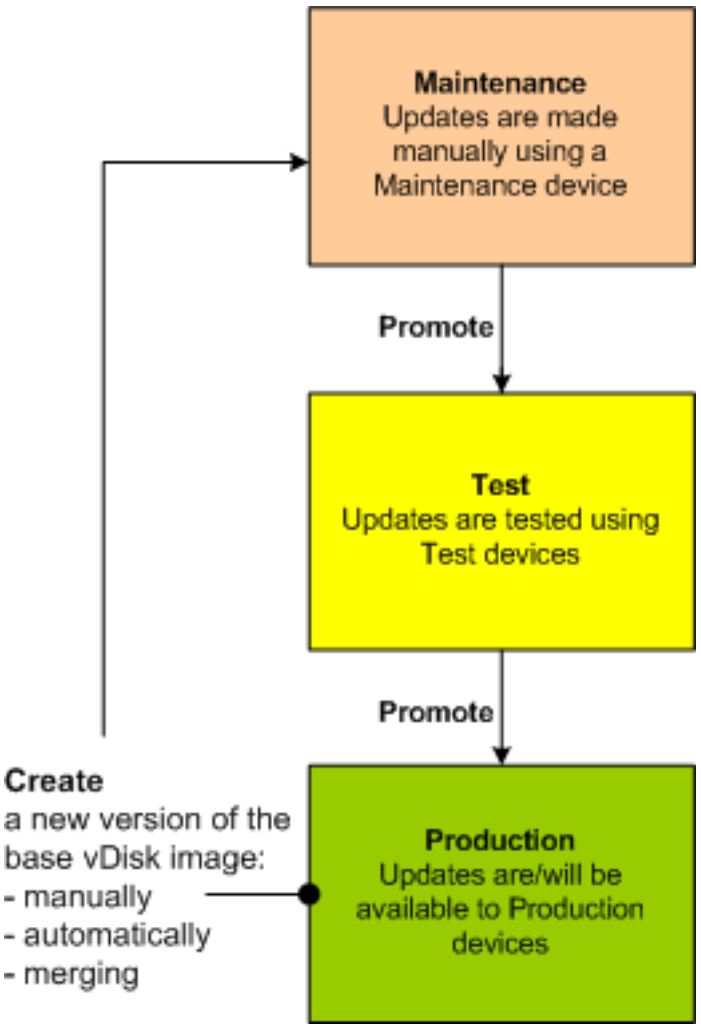
August 21, 2018

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 (VHDX file). 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. Availability also depends on the type of device attempting to access it, for example, Maintenance Device, Update Device, Test Device, or Production Device.

If you are updating a device that uses a personal vDisk image, ensure compatibility in your production environment using this procedure:

Note: If you are updating images for devices that use a personal vDisk, it must be done on a virtual machine without a personal vDisk. Otherwise, updates are saved to the personal vDisk image rather than the virtual machine image.

1. Create a maintenance version of the vDisk.
2. Make any necessary updates to the maintenance version.
3. Promote the new maintenance version to test.
4. Boot the PvD test device, and verify updates.
5. Promote the test version to production.

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 Versioning dialog indicates that the newly created version is in maintenance. While under maintenance, this version is updated by a single Maintenance device. 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 updating automatically, the Access column on the vDisk Versioning dialog indicates that the newly created version is in maintenance. In maintenance mode, this version is updated by the device to which it is assigned (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. Attempting to register 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 illustrates 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 table below illustrates these chain sequences:

	VHDX Filename	Properties Filename	Lock File Filename
Base Image	win7dev.vhdx	win7dev.pvp	win7dev.lok
Version 1	win7dev.1.vhdx	win7dev.1.pvp	win7dev.1.lok
Version 2	win7dev.2.vhdx	win7dev.2.pvp	win7dev.2.lok
…	…	…	…
Version N	win7dev.**N**.vhdx	win7dev.**N**.pvp	win7dev.**N**.lok

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. Refer to 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.

> **Note:**
>
> Updating images for devices that use a personal vDisk, must be done on a virtual machine that does not have a personal vDisk attached. Otherwise, updates are saved to the personal vDisk image rather than the virtual machine image.

Create a version

1. In the 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 with 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. This process does not work if the device is a PvD Test device.

4. Select the vDisk, then right-click. Select the **Promote...** menu option from the context menu that appears (for more details on promoting versions refer to 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 virtual disk 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 virtual disk only occurs when a Maintenance version is not defined, or when it is in Private Image mode. A merged virtual disk starts from the top of the chain down to the base disk image. A starting disk cannot be specified for the merged virtual disk.

Merging to a New Base Image

A full merge to a new base image combines a chain of differencing disks and base image disks into a new single base disk. This new disk is the next version in the chain, with the file 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 (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 may be 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, refer to 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.

Configure an automatic consolidation of differencing disks in the Farm Properties dialog's virtual disk Version tab. On this tab, select a maximum virtual disk number. When that number is reached, a merge is automatically performed. The availability of that virtual disk 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 virtual disk in the Console, then select the **Versions** menu option. The virtual disk **Versions** dialog appears.
2. Click the **Merge** button. The Merge dialog appears.
3. Select to perform a **Merged Updates** or **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 virtual disk mode defaults to **automatic range**, specified in the Farm Properties virtual disk 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 virtual disk 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 to allow maintenance devices to make updates (read/write). After you finish update, this version can be promoted from Maintenance to Test (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:**
>
> If Access displays as blank, this version is considered released to production but is not the version currently selected from which devices should boot.

Updating vDisks on target devices

This document 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 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 should be 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 may execute every day. These updates are automatically made whenever you add new vDisk 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. Determine if the update is immediately applied, or on a scheduled date when checking for updates by running the **ApplyAutoUpdate**.

   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, then set the following vDisk properties:

   a. Only enable automatic updates if this vDisk may later be replaced with 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. Refer to '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. Refer to Enabling Automatic vDisk Updates.
2. Configuring a Virtual Host Pool for Automated vDisk updates. Refer to Using the Virtual Host Connection Wizard. Note: Supported hypervisor types include; Citrix XenServer, Microsoft SCVMM/Hyper-V, and VMWare vSphere/ESX.
3. Create and configure an ESD VM that used to update the vDisk. Refer to Creating and Configuring ESD Update VMs.
4. Configuring vDisks for Automated updates. Refer to the Using the Managed vDisk Setup Wizard.

5. Creating and managing update tasks. Refer to 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 will boot, 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. Refer to *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\ProvisioningServices
- Create a string value in the PlatformEsx key named ServerConnectionString and set it to http://%7B0%7D:PORT#/sdk (If you are using port 300, ServerConnectionString= http://%7B0%7D:300/sdk)

To configure virtual host connections:

1. Under the vDisk Update Management node in the Console tree, 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 Microsoft, 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 hostname or the IP address of the server to contact. If an ESX hypervisor was selected, optionally specify the datacenter 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: Username – 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 hostname 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\ProvisioningServices\PlatformEsx. Or, create a string in the PlatformEsx key named 'ServerConnectionString' and set it to http://%7B0%7D:PORT#/sdk (If you are using port 300, ServerConnectionString= http://%7B0%7D:300/sdk)
Datacenter	Optional. If an ESX hypervisor was selected, optionally specify the datacenter 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.

Field	Description
Password	The account password that is associated with the username. The password must be a maximum of 32 characters.
Verify Connection Button	Click this button to verify that the username 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.

Retiring or deleting vDisks

August 15, 2018

When a vDisk is no longer needed, it can be retired. Retire a vDisk by deleting it. When a vDisk is deleted, all VHDX differencing disk files, properties files, lock files, and 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. If you are deleting a personal vDisk, a confirmation dialog appears. This warning indicates that you are deleting the vDisk reference files as well as the device to which it is assigned.

To delete a vDisk

1. In the 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 checkbox for deleting the vDisk from the hard drive option. Or, do not select the checkbox to delete the vDisk from the store and database. Unless a backup copy is made before deleting a vDisk image file from the store, the vDisk image file is permanently deleted.
4. Click Yes. The vDisk is deleted.

Printers

July 2, 2018

Provisioning Server provides a Printer Management feature that allows you to manage which printers target devices have access to on a vDisk. Printers are managed from the Target Device Properties dialog.

This feature should not be enabled if you use Active Directory to manage printers. If you use an existing printer management tool, this feature should be disabled to avoid printer setting conflicts.

Printers can only be added to the top-level differencing disk version while it is under Maintenance or if it is a Private Image. If a device boots from a previous version, the printer configuration may not match.

There are two types of printers that can appear in the Console window:

- Network Printers
- Local Printers

Before a target device can access a printer, the following tasks must be completed in the order that follows:

- Installing Printers on the vDisk
- Enabling Printers on the vDisk
- Enabling the Printer Management Feature

Installing printers on a vDisk

Printers must be installed on the vDisk image before the printers are available to target devices booting from that disk. Printers can only be added to the top-level differencing disk version while it is under Maintenance or if it is a Private Image. If a device boots from a previous version, the printer configuration may not match.

To install printers on the vDisk

1. Change the vDisk image mode to Private Image mode.
2. Install the required printers on the target device that is using the vDisk.
3. Perform a clean shut-down of the target device that is using the vDisk.
4. If this vDisk is shared by users, change the vDisk image mode back to Shared Image mode.
5. Verify that the printers display in the Console:
    a) Right-click on the target device, select the Properties menu option.
    b) Select the vDisks tab, then click on the Printers button. Printers associated with that vDisk should appear in the list of available printers.

After successfully installing printers, the next step is to enable printers for target devices that access this vDisk.

Enable or disable printers on a vDisk

By default, printers are not enabled on the vDisk. Enable or disable printers from the Target Device Properties vDisk tab. On the Printers dialog, enable the checkbox next to each printer to enable or disable it. After enabling (assigning) printers to target devices, the Printer Management feature must then be enabled on the vDisk.

Until Printer Management is enabled, all printers that are installed on the target device are available to that target device. By enabling Printer Management, you can select printers or remove printers from individual target devices.

> **Note:**
>
> The Printer Management feature is only recommended if you are not using Active Directory to manage printer groups.

After a target device boots, printer information, which is included in a vDisk image, becomes available to target devices. Printer Management is initially disabled until all printer-to-target device assignments are completed for the vDisk. Disabling individual printers prohibits target devices from accessing those printers.

> **Tip:**
>
> Disabling printers does not remove the printer information from the vDisk. Changes to the target devices printer assignments do not occur until the target device reboots.

Examples of reasons you may want to disable Printer Management include:

- You may be using a different printer system that installs the valid printers on each target device and software may delete them or cause conflicting settings.
- Printers that are included on the vDisk should be accessible to all users.
- The system needs to be configured before being deployed. Until the Printer Management feature is enabled, changes can be made for different target devices as needed.

All printers installed on a vDisk appear in the Details panel when the Printers group folder is expanded for that vDisk.

If a disk is a HA vDisk (has a duplicate with same vDisk name), changes to that printer (if it is enabled or disabled for a target device) are automatically made to the duplicate vDisk.

Enablement methods

Using the Console, you can manage which target devices use which printers. There are several methods for managing target device printer assignments. Choose from the following methods:

- Enabling printers for target devices using the Printer settings option. Use this method to enable or disable a single printer to multiple target devices accessing a vDisk.
- Enabling printers for target devices using the Printers group folder. Use this method to select printer settings (enable/disable; default) for a single target device.
- Enabling printers using Copy and Paste. Use this method to copy printer settings of one target device (enabled/disabled; default printer), to one or more target devices selected in the Details panel.
- Enabling printers using an existing target device as a template. Use this method to automatically set printer settings when a target device is added to the network.

> **Note:**
>
> The Administrator may choose to limit the number of printers for particular target devices or select different default printers for particular target devices. The settings that are selected are saved to the target device's personality information (if the limit for this field, 65K, is reached, a message appears indicating that some of the settings will not be saved and offers suggestions for decreasing the size).

Using the Console, you can manage which target devices use which printers. There are several methods for managing target device printer assignments. Choose from the following methods:

- Enabling printers for target devices using the Printer settings option. Use this method to enable or disable a single printer to multiple target devices accessing a vDisk.
- Enabling printers for target devices using the Printers group folder. Use this method to select printer settings (enable/disable; default) for a single target device.
- Enabling printers using Copy and Paste. Use this method to copy printer settings of one target device (enabled/disabled; default printer), to one or more target devices selected in the Details panel.
- Enabling printers using an existing target device as a template. Use this method to automatically set printer settings when a target device is added to the network.

Methods for enabling printers on a vDisk

Enabling printers for target devices using the Printer Settings option

Use this method to assign a single printer to multiple target devices. This method is very useful when managing the printer-to-all target devices relationship.

1. In the Console tree, under Provisioning Servers, click the Printers group folder. All printers associated with that group appear in the Details panel.
2. Right-click on a printer in the Details panel, then select the Client Printer Settings menu option. The printer settings dialog for that printer appears.
3. Enable or disable this printer for one or more target devices using either of the following options:
    - In the Enable column, select the check box next to each target device to enable or disable use of this printer.
    - Select the check box under the dialogs Enable heading to enable or disable this printer for all target devices assigned to the vDisk.
4. To select this printer as the default printer for target devices accessing this vDisk, select from the following methods:
    - Select the Defaultcheck box in the dialogs Default heading to set this printer as the default for all target devices assigned to this vDisk.
    - Highlight one or more target devices, then right-click to open the context menu. Select from the following menu options; Default,NotDefaultAll DefaultAll Not Default
    - In the Default column, select the check box next to each target device that should use this printer as the default printer. If there is only one printer, that printer is automatically set as the default printer.
5. Click OK to save settings for this printer and exit the dialog.

Enabling printers for target devices using the Printers group folder

Use this method to select printer settings (enable/disable; default) for a single target device.

1. Under the target device vDisk, click the Printers group folder in the tree. Printers that are associated with that group appear in the Details panel. By default, printers are not enabled for a target device and the first printer listed is set as the default printer.
2. Select or deselect the Enable check box next to each printer to enable or disable the printer for this target device. You can also choose from one of the additional selection methods that follow.

   In the Details panel:

   - Select or unselect the Enable check box within the table heading to enable or disable all printers.
   - Highlight a printer, then use the space bar to enable or disable printers.

> **Tip:**
>
> After selecting printer settings for a single target device, you can duplicate these settings using the Copy and Paste features.

Enabling printers using Copy and Paste

Use this method to set the printer settings (enabled/disabled; default printer) that exist for one target device for other target devices that use the same vDisks. This method is particularly useful when adding new target devices.

1. In the Console, right-click the target device that you want to copy printer settings from.
2. Select the Copy menu option. The Copy target device properties dialog appears.
3. Under Options, select Printers, then click OK to exit the dialog.
4. In the Tree, highlight the Target Devices directory so that all target devices appear in the Details panel.
5. Highlight one or more target devices that you want to paste the printer settings to (enable/disable; default).
6. Right-click the highlighted target devices, then select the Paste menu option.

Enabling printers using an existing target device as a template

Use this method if you want all new target devices that are added to your network to automatically share printer settings (enable/disable; default).

1. In the Console, double-click the target device that you want to select as the template. The Target Device Properties dialog appears.
2. On the General tab, select the Set as default target device option.
3. Click OK to exit the dialog.

Enabling the Printer Management feature

After assigning printers to target devices, the Printer Management feature must be enabled before any printers on the target device can be removed. Until Printer Management is enabled, all printers installed on the target device are available to the target device. Once the feature is enabled, any changes to target devices printer settings (enable/disable; default) become available the next time the target device boots from the vDisk.

> **Important:**
>
> The Printer Management feature is only recommended if you are not using Active Directory.

If the Printer Management feature is disabled and a target device boots from a vDisk that has printers installed on it, that target device has access to all printers on that vDisk. If the Printer Management feature is enabled and the target device boots from that same vDisk, that target device can only access those printers that are enabled for that target device.

To enable or disable printers on a selected vDisk

1. In the Console, expand the Provisioning Server node in the tree panel, then select the vDisk that you want printers enabled or disabled on.
2. Select File Properties from the right-click menu, then select the Options tab.
3. Under Printer Settings, select the Enable the Printer Settings check box option to enable settings, or leave the check box blank to disable printer settings.
4. If the Enable the Printer Management check box is selected, the Enable Printer Management menu options appear checked when the Printers group is highlighted.
5. If the Enable the Printer Management check box appear disabled, all printers exist on the selected vDisk.

You can also choose from the following methods to enable or disable the Printer Management feature using right-click menus:

- **Printers Group** - In the Tree, under Provisioning Servers, expand a Provisioning Server, then expand the vDisk for which you want to disable Printer Management. Right-click on the Printers folder for that vDisk, then select the Disable Printer Management option.
- **Virtual Disk** - In the Tree, under Provisioning Servers, right click on the vDisk for which you want to disable Printer Management, then select the Disable Printer Management option.

Views

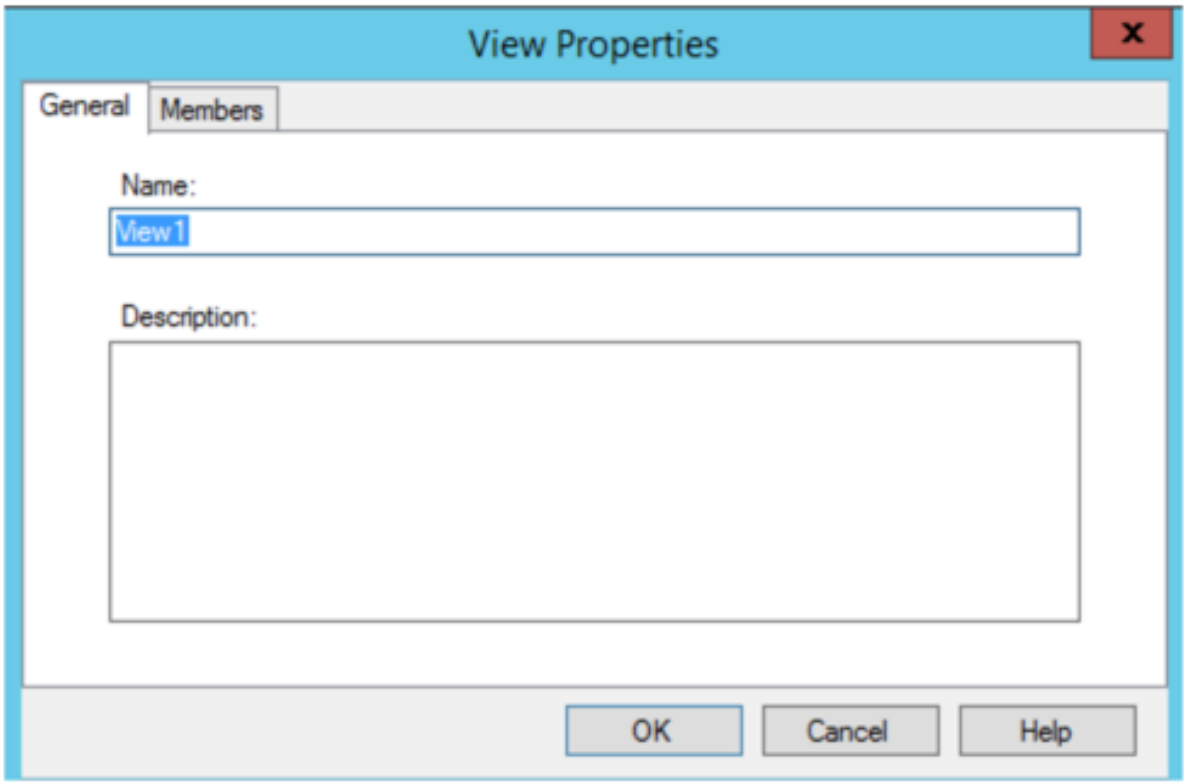
August 8, 2018

The 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 can create and manage views in the Console tree's Farm > Views folder. Farm views can 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 and allows you to view or make modifications to that view.



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.

Managing views in the console

Creating a View

1. In the Console, right-click on the Views folder where the new view will exist, 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 and a description of this view in the Description text box, 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 drop-down menus, select the site, then the device collection that you want to add target device(s) 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 additional 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.

Pasting Device Properties

To copy the properties of one target device, and paste those properties to target device members within a view, complete the steps that follow.

To 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 checkbox 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 will inherit the copied properties, then select the Paste device properties menu option. The Paste Device Properties dialog appears displaying the name and properties of the target device that were copied.
4. Under the Paste to table heading, highlight the target devices that will inherit these properties, then click Paste.
5. Click Close to close the dialog.

Deleting 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.

Refreshing a View

After making changes to a view, it may be necessary to 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.

Booting 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 drop-down 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.

Restarting 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 drop-down 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 drop-down 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 shutdown 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 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 drop-down 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

July 2, 2018

The ability to view and manage objects within a Provisioning Server implementation is determined by the administrative role assigned to a group of users. Provisioning Services makes use of groups that

already exist within the network (Windows or Active Directory Groups). All members within a group will share the same administrative privileges within a farm. An administrator may have multiple roles if they belong to more than one group.

The following administrative roles can be assigned to a group:

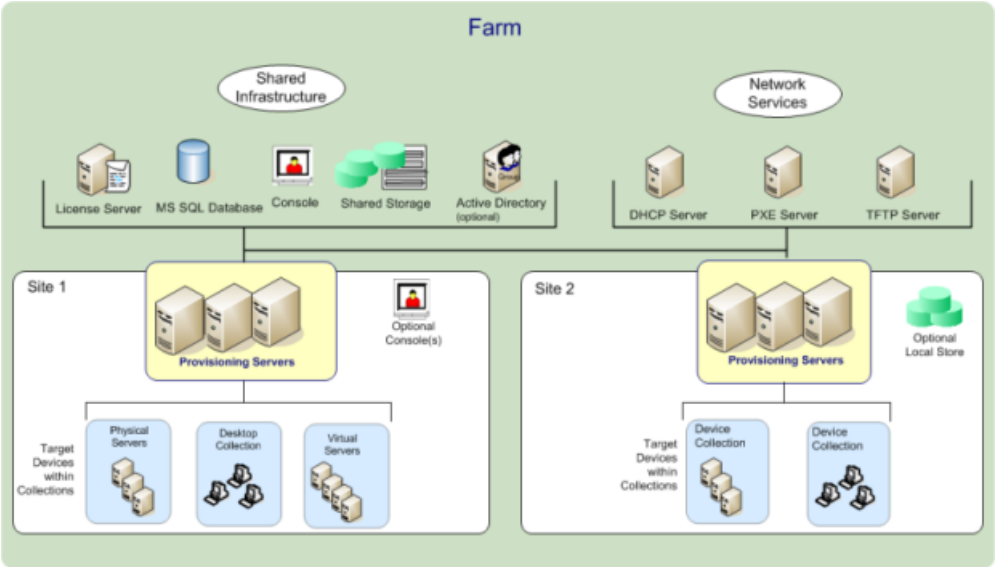
- Farm Administrator
- Site Administrator
- Device Administrator
- Device Operator

After a group is assigned an administrator role through the Console, if a member of that group attempts to connect to a different farm, a dialog displays requesting that a Provisioning Server within that farm be identified (the name and port number). You are also required to either use the Windows credentials you are currently logged in with (default setting), or enter your Active Directory credentials. Provisioning Services does not support using both domain and workgroups simultaneously.

When the information is sent to and received by the appropriate server farm, the role that was associated with the group that you are a member of, determines your administrative privileges within this farm. Group role assignments can vary from farm to farm.

Managing farm administrators

Farm administrators can view and manage all objects within a farm. Farm administrators can also create new sites and manage role memberships throughout the entire farm. In the Console, farm-level tasks can only be performed by farm administrators. For example, only a farm administrator can create a new site within the farm.



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 the Configuration Wizard is run, additional groups can be assigned the Farm Administrator role in the Console.

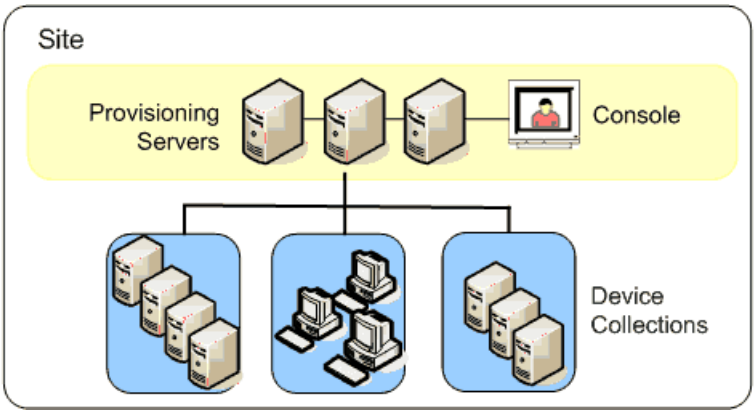
To assign additional Farm Administrators

1. In the Console, right-click on the farm to which the administrator role will be assigned, then select Properties.The Farm Properties dialog appears.
2. On the Groups tab, highlight all the groups that will be assigned administrative roles in this farm, then click Add.
3. On the Security tab, highlight all groups to which the Farm Administrator role will be assigned, the click Add.
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.

Managing site administrators

Site administrators have full management access to all the objects within a site. For example, the site administrator can manage Provisioning Servers, site properties, target devices, device collections, vDisk assignments and vDisk 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 tasks such as adding and removing vDisks 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 will be 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 drop-down menu, select each group to associate with the site administrator role, then click OK.
4. Optionally, repeat steps 2 and 3 to continue assigning additional 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 vDisks from a device, editing device properties and viewing vDisk Properties (read-only). Device collections consist of a logical grouping of devices. For example, a device collection could 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 tree, 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. To assign a group with the device administrator role, select each system group that should have device administrator privileges, then click OK.
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 tree, 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 should have device operator privileges, then click OK.
5. Click OK to close the dialog box.

Enable SQL Server Always On multi-subnet failover

August 22, 2018

Citrix Provisioning supports SQL Server AlwaysOn failover in multi-subnet environments. The database server is accessed via ODBC which requires the SQL Server Native Client as a pre-requisite of the Provisioning Server software.

Ensure that the Provisioning Server is connecting to an AlwaysOn availability group listener containing the Failover Cluster Instance when enabling MultiSubnetFailover.

> **Tip:**
>
> The SQL Server Native Client is part of the Citrix Provisioning installer. No additional installation procedures are necessary to use this functionality.

This feature is enabled using the **Enable MultiSubnetFailover for SQL** field on the **Database Server** page in the Provisioning Services Configuration Wizard.

> **Note:**
>
> For more information, refer to SQL AlwaysOn for SQL Server 2012 and 2014.

To enable SQL server always on in multi-subnet environments

1. After launching the Citrix Provisioning Configuration Wizard, access the **Database Server** screen.
2. In the Database Server screen:
   - Specify the AlwaysOn availability group listener in the Server name field.
   - Specify the Instance name.
   - Optionally specify the TCP port number.

3. Select the **Enable MultiSubnetFailover for SQL Server Always On** checkbox.
4. Click **Next** to continue with the configuration wizard.

Managing for highly available implementations

August 22, 2018

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 Provisioning Servers to use a snapshot of the database if the connection to the database is lost.
  - Database Mirroring.
- Provisioning Servers
  - Provisioning Server Failover. If a server becomes unavailable, another server within the site can provide active target devices with the vDisk.

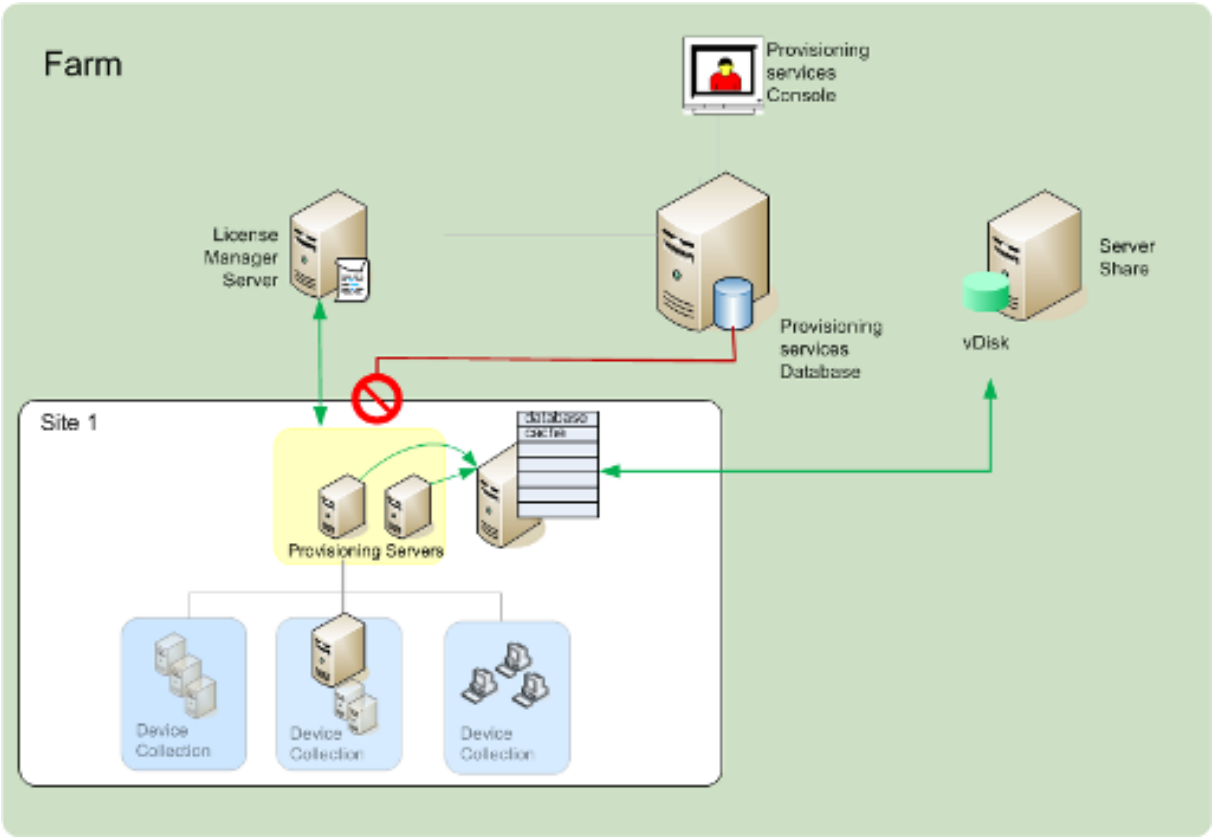
  - Managing Servers. You can load balance between Provisioning Servers to prevent overload and to allow server capacity to be used more effectively and efficiently.
- vDisks and Storage
  - Configuring Highly Available Shared Storage

Offline database support

July 30, 2018

When offline database support is enabled on the farm, a snapshot of the database is created and initialized at server startup. It is then continually updated by the Stream Process. If the database becomes unavailable, the Stream Process uses the snapshot to get information about the Provisioning Server and the target devices available to the server; this allows Provisioning Servers and target devices to remain operational. However, when the database is offline, Citrix Provisioning management functions and the Console become unavailable.

When the database connection becomes available, the Stream Process synchronizes any Provisioning Server or target device status changes made to the snapshot, back to the database.



Considerations

The following features, options, and processes remain unavailable when the database connection is lost, even if the Offline Database Support option is enabled:

- AutoAdd target devices
- vDisk updates
- vDisk 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 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

August 29, 2018

In order to provide a highly available configuration, if you mirror a MS SQL database and the primary version becomes unavailable, Citrix Provisioning supports the mirrored version. This results in improved overall availability of Citrix Provisioning.

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 the failover server be up and running before enabling database mirroring in the farm. For helpful information on configuring the MS SQL failover server, refer to https://technet.microsoft.com/en-us/library/ms188712.aspx.

The procedures that follow are only intended to call out the steps that are applicable to database mirroring when running 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 re-running the wizard, some services, including the stream service, restart so that the farm has the new failover server settings specified with the wizard was run.

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 page displays, select the **Create Farm** radio button to create a new farm, then click Next.
3. Type or use the Browse button to identify the primary database server and instance names. Optionally, enter a TCP port number to use to communicate with this database server.
4. Enable the Specify database mirror failover partner option.
5. 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.
6. Click Next. If the failover database has already been configured and it is up and running, Citrix Provisioning should be able to connect to it. If the failover database server has not yet been created or is not running, an error message may display 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).
7. On the New Farm page, enter a name for the new database on the primary database server, then complete any additional requested information.
8. Click Next.
9. 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 exisiting farm option on the Farm Configuration page.
5. On the Database Server page, select the primary and failover database servers and instance names, then enable the database mirror failover feature .
6. Complete the remaining wizard pages.

SQL AlwaysOn for SQL Server 2012, 2014, and 2016

July 30, 2018

Citrix Provisioning supports the SQL AlwaysOn high availability and disaster recovery solution. Consider the following:

- The SQL 2012 native client is required. This is an optional prerequisite in the Citrix Provisioning server install process.
- Citrix Provisioning is only aware of and interacts with AlwaysOn 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 AlwaysOn. Citrix Provisioning is not responsible for this.
- The soap/stream services user must be manually configured to have full permission to each SQL server part of the AlwaysOn configuration.
- Citrix Provisioning is not aware of the individual SQL server/cluster behind SQL AlwaysOn.

> **Note:**
>
> Refer to Supported Databases for XenApp and XenDesktop Components in the Knowledge Center for additional information about supported databases and clients.

Provisioning Server failover

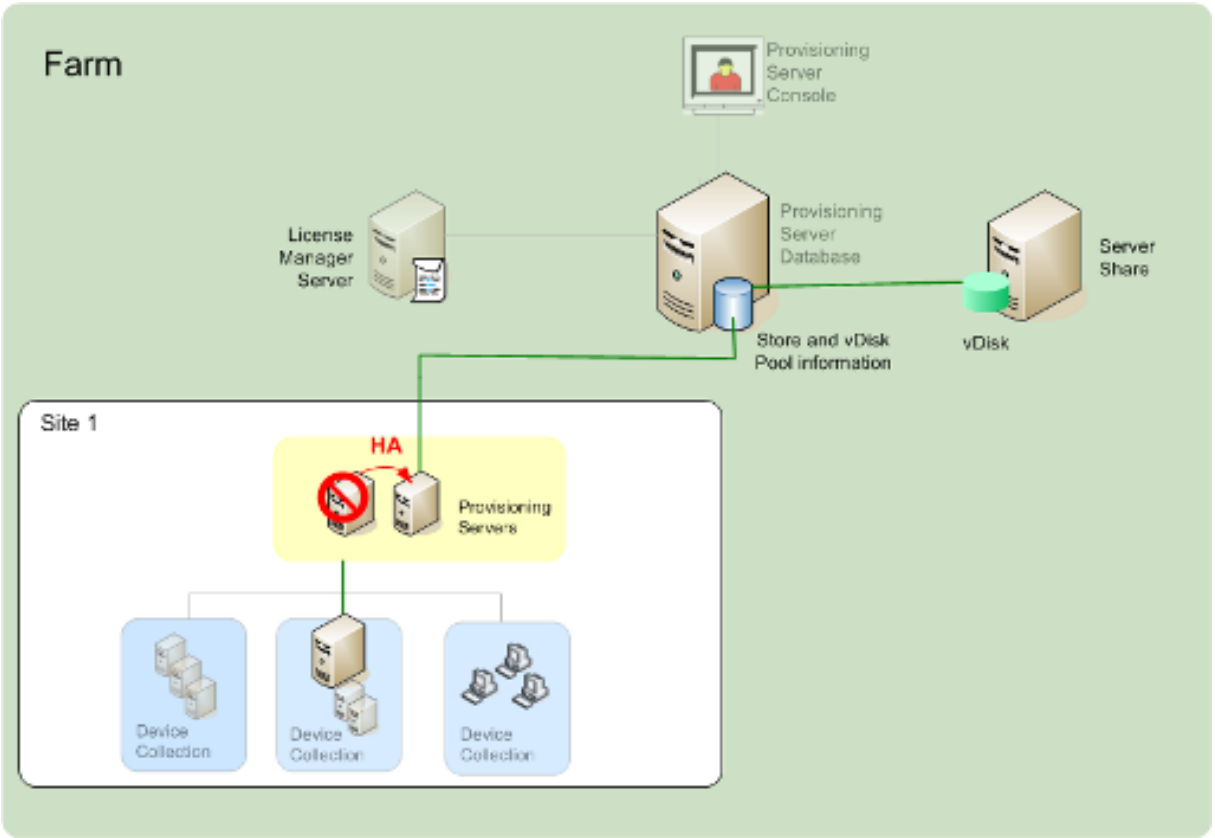
August 15, 2018

By default, all Provisioning Servers within a site that can access a vDisk provide that vDisk to target devices. On shared storage, multiple Provisioning Servers access the same physical files, allowing a target device to establish a connection on an alternate Provisioning Server. This *failover* permits a connection to the active Provisioning Server is 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 vDisk provide that vDisk to target devices. For example, if a vDisk is replicated across three servers and one of the vDisks is updated, that vDisk 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 vDisks, the timestamps on each differ, resulting in vDisks that are no longer identical.
>
> Provisioning Services does not support vDisk high availability on local storage in Private Image mode or that are currently in maintenance mode.

If load balancing is enabled and a server providing that vDisk fails, the load is automatically balanced between the target device and the remaining servers. If the load balancing option is not enabled, a single server is assigned, providing the vDisk to target devices. In such situations failover does not occur.

For information on automatically balancing the target device load between servers, refer to Managing Servers.



The Provisioning Server accessed by the target device does not necessarily become the one that accesses the vDisk on behalf of it. In addition, once connected, if one or more servers can access the vDisk 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 Provisioning Server.
2. Right-click the connected Provisioning Server in the Console. Select Stream Services, then select Stop.
3. Confirm that the IP address of the connected server changes to that of an alternate server in the vDisk status dialog.

Configuring for high availability with shared storage

August 29, 2018

Provisioning Servers are configured to access your shared-storage location. Citrix Provisioning supports various shared-storage configurations. The configuration steps for highly available storage in the network varies depending on shared-storage configurations.

> **Warning:**
>
> Installing Provisioning Services affects the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters\OplocksDisabled. Changing this registry key disables Windows Opportunity Locking, providing the fastest possible failover time when contact with the active Provisioning Server is lost. Without this change, failover times can take up to one minute. During this time, Windows does not allow access to the vDisk file that was in use by the failed Provisioning Server. By disabling Windows Opportunity Locking on Provisioning Servers, the Stream Service can have immediate access to vDisk files. However, this reduces caching of remote vDisk data for the entire Provisioning Server.

Windows shared-storage configuration

If you are using a Windows shared-storage location, the Service account credentials (user account name and password) must be a domain account that is configured on each Provisioning Server, in order 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 vDisk stored locally on the Provisioning Server, the local user rights provide full access. However, when the database or vDisk is located 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 Provisioning Servers that will participate in HA. 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, as well as 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 PVS 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 need to be shared, and the Service account credentials need to have access to remote storage for vDisks, with the appropriate permissions.

To share your vDisk'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 vDisk folders. For example, if the database and vDisk 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 check boxes below it should be checked).
9. Click Apply.
10. Click 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 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 may not be necessary to guarantee access to your data.

In most cases, a SAN configuration allows setting up as if the database and vDisks were stored locally on the Provisioning Server.

Configuring the boot file for high availability

August 30, 2018

When a Provisioning Server is configured by the Configuration Wizard, that server can be selected as one of the servers used to connect target devices during the boot process. To be highly available, at least two login Provisioning 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 Provisioning Servers, as well as other configuration information. The boot file lists the Provisioning Servers that a target device can contact to get access to the Citrix Provisioning farm. The server that is contacted may hand the target device off to a different Provisioning Server that is able to provide the target device with its vDisk.

> **Note:**
>
> A shared storage system ensures the availability of the 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 Provisioning Servers to the boot file

You must add Provisioning Servers to the boot file in order to provide a target device with the information necessary to make contact with the Stream Service.

When first configuring a Provisioning Server, the Configuration Wizard allows you to select the server, which is currently being configured, to provide TFTP services. If all target devices are on one network segment, there will typically be 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) may be used.

Provisioning Servers can also be configured as login servers in the Console using the Configure Bootstrap dialog.

Select from either method to add Provisioning Servers to the boot file.

Adding Login Servers using the Configuration Wizard

To add and configure the first Provisioning Server as the TFTP and login server using the Configuration Wizard:

1. Run the Configuration Wizard and when presented with the TFTP option and bootstrap location dialog, select the **Use the Provisioning Server TFTP Service** option.
2. Enter or browse for the bootstrap file location, then click **Next**. The default location is: C:\Documents and Settings\All Users\Application Data\Citrix\Provisioning Services\Tftpboot

   > **Note:**
   >
   > If a previous version of Provisioning Server was installed on this server, you may need to change the default location from C:\Program Files\Citrix\Provisioning Server\TFTPBoot or C:\Documents and Settings\All Users\Application Data\Citrix\Provisioning Server\TFTPboot to: C:\Documents and Settings\All Users\Application Data\Citrix\Provisioning Ser-

> vices\TFTPboot. If the default is not changed, the bootstrap file can not be configured from the Console and target devices will fail to boot; the Missing TFTP error message appears.

3. In the Provisioning Servers boot list, click **Add** to add additional login Provisioning Servers to the list. Use the Move up or Move down buttons to change the Provisioning Server boot preference order.

   > **Note:**
   >
   > In an HA implementation, at least two Provisioning Server must be selected as boot servers.

4. To set advanced configuration settings, highlight the IP address of the Provisioning Server, click Advanced, then configure the bootstrap file. For field definitions, refer to Provisioning Server Properties.
5. Click OK, then click Next.
6. Review the configuration settings, then click Finish to confirm configuration settings and restart network services on this server. As configuration settings are saved, they display in the progress dialog.
7. To exit the Configuration Wizard, click Done.

Adding Login Servers Using the Console

To add and configure additional Provisioning Servers as a login servers:

1. In the Console, right-click on a Provisioning Server that will be used as a login server, then select the **Configure Bootstrap** menu option. The Configure Bootstrap dialog appears.

   > **Note:**
   >
   > Clicking **Read DB** populates the table with login servers that already exist. When the Stream Service starts, it creates a record in the database with its own IP address. There is only one Stream Service option record per database. If the service is bound to multiple IP addresses, multiple records appear in the database. The Read DB function chooses only one IP address from each Provisioning Server. This function can also be used to populate the boot file with the Stream Service IP settings already configured in the database.

2. Click **Add** to add a new login Provisioning Server to the bootstrap file. The Streaming Server dialog appears.
3. Type the IP address and port number of this Provisioning Server in the appropriate text boxes.

4. Select to either use subnet mask and gateway settings using DHCP/BOOTP, or type in the settings to use, then click OK. The Provisioning Server information displays in the list of available login servers.
5. To configure advanced bootstrap settings, on the Options tab, choose from the following settings:
    - Select **Verbose Mode** if you want to monitor the boot process on the target device (optional). This 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** checkbox unless you are using older versions without PAE enabled.
6. 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 Provisioning Server.

      > **Note:**
      >
      > Because the **Seconds** field does not apply, it becomes inactive when the Restore Network Connections option is selected.

    - Reboot to Hard Drive - 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. Determine the number of seconds to wait before rebooting. Assuming the network connection can not be established, PXE will fail and the system will reboot to the local hard drive. The default number of seconds is 50.
7. Under Timeouts, scroll for the Login Polling Timeout, in milliseconds, between retries when polling for Provisioning Servers.
8. Under Timeouts, scroll for the Login General Timeout, in milliseconds, for all login associated packets, except the initial login polling time-out.
9. Click OK to save your changes.

Troubleshooting

August 9, 2018

Use the information in this section to troubleshoot Citrix Provisioning components:

- Logging
- Auditing
- APIs
- CIS Problem Reporting

Logging

August 29, 2018

Citrix Provisioning uses Citrix Diagnostic Facility (CDF) tracing for troubleshooting and managing a Provisioning Services farm.

Use the PVSDataCollector v2.0.0 tool to collect all Citrix Provisioning data, including the ETL log. For details, refer to http://support.citrix.com/article/CTX136079.

To generate a Citrix Provisioning ETL log, you must install the CDF monitor. For details on installing the monitor, refer to: http://support.citrix.com/article/CTX138698.

To review ETL logs using CDF, refer to http://support.citrix.com/article/CTX111961.

Always on Tracing

Citrix Provisioning updated Always on Tracing (AOT) functionality. In previous releases, AOT logs were stored in the memory of the Provisioning Server. In the event of a crash, the Server would lose these log files. To resolve this issue, Citrix Provisioning now allows you to store AOT logs directly to disk. The administrator can use PoSH on the Provisioning Server to configure this functionality.

Consider the following:

- By default, this functionality is enabled.
- The default disk size is 500 MB.
- AOT logs are saved in C:\ProgramData\Citrix\Provisioning Services\Log\AOT.
- Use PoSH commands to modify or disable the feature.
- This functionality records CPU and IOPS.

Saving AOT logs to disk

Use the **Enable-CitrixTrace** Powershell telemetry command to allow Citrix Provisioning to save trace files on disk at a given persistDirectory. The maximum size of the trace files (in bytes) stored is configured using the **maxSizeBytes** parameter. The **sliceDurationSeconds** parameter defines the duration, in seconds, of the slice/block trace.

The syntax for this command is:

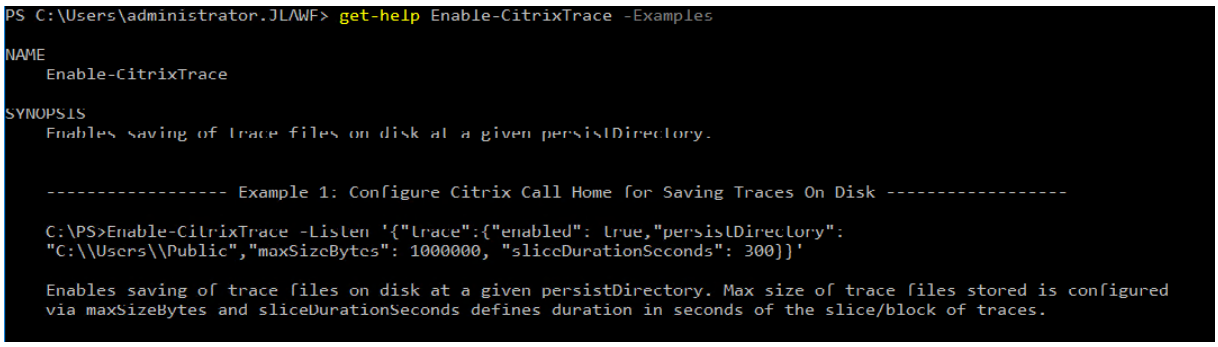
```
    Enable-CitrixTrace -Listen

    '{
"trace":

```



```
    {
  ”enabled”: true,

    ”persistDirectory”:”C:\ProgramData\Citrix\Provisioning Services\Log
       \AOT”,

    ”maxSizeBytes”: 524288000,

    ”sliceDurationSeconds”: 300

     }


     }
  ’
```

For example:

```
C:\PS>Enable-CitrixTrace -Listen  ‘{
  “trace”  :{
  “enabled” : true,  “persistDirectory” :  “C:\Users\Public” ,”
    maxSizeBytes” : 1000000,  “sliceDurationSeconds” : 300 }
  }
  ’
```



Auditing

August 22, 2018

Citrix Provisioning provides an auditing tool that records configuration actions on components within the provisioning farm, to the provisioning database. The auditing tool provides administrators with a way to troubleshoot and monitor recent changes that might impact system performance and behavior.

Administrator privileges determine the audit information that can be viewed and the menu options that are visible. For example, a Farm Administrator can view all audit information within the farm. This functionality is unlike a Device Administrator who can only view audit information for those device collections for which they have privileges.

> **Note:**
>
> Auditing is off by default. If the provisioning database is unavailable, no actions are recorded.

To enable auditing

1. In the 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:

- Console
- MCLI
- SOAP Server
- PowerShell

Accessing auditing information

Auditing information is accessed using the 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 audit information. The audit information that other administrators can access depends on the role they were assigned.

The tree allows for a drill-down approach when accessing the level of audit information needed.

To access auditing information from the console

1. In the 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, which 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 or 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 drill down to view secondary object actions such as Parameters, Sub Actions, and Changes as described below.
    - **Parameters:** Any other information used to process the action. This option opens the Parameters dialog, which includes Name (parameter name) and Value (object name) information.
    - **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 Name, Old, and New information.

Archiving audit trail information

The Farm Administrator determines how long to make audit trail information accessible before it is archived.

To configure audit trail archiving

1. In the Console tree, 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** drop-down menu, then select the date on which the audit trail information should be 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

September 12, 2018

There are four APIs available with Citrix Provisioning. Each API has its own Programmer's Guide. There is also a guide on how to manage the transition between the deprecated PowerShell API and the object-oriented PowerShell API.

- Object-oriented PowerShell interface: PowerShell with Object Programmer's Guide
- Deprecated PowerShell interface: PowerShell (Deprecated) Programmer's Guide
- Managing the transition between the deprecated PowerShell interface and the object-oriented PowerShell interface: Transition to PowerShell with Objects from PowerShell (Deprecated) Programmer's Guide
- SOAP Server interface: SOAP Server Programmer's Guide
- MCLI interface: MCLI Programmer's Guide

Active Directory group enumeration method

The Citrix Provisioning Console contains the Citrix Virtual Apps and Desktops Setup Wizard. It provides integration tasks between

Citrix Provisioning, Citrix Virtual Apps and Desktops and Windows Active Directory. The Wizard, accessible from the Provisioning Console, 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 could not execute 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 that 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 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>.
3. Run the following commands:

   a. Create a certificate to act as your root certificate authority: **makecert -n "CN= P VSRoot CA" -r -sv P VSRoot CA.pvk P VSRoot CA.cer**
   b. Create and install the service certificate: **makecert -sk P VSAP I -iv P VSRoot CA.pvk -n "CN= FQDN of the PVS Server" -ic P VSRoot CA.cer -sr localmachine -ss my -sky exchange -pe**
   c. 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**
4. Run the Configuration Wizard. On the **Soap SSL Configuration page**, select the created certificate.

> **Note:**
>
> When you run the **PowerShell** commands, use the *FQDN of the PVS Server* for **PvsServerAddress** and 54324 (default) for **PvsServerPort**.

Using 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.

1. Open a **PowerShell** window on your Provisioning Server:

   a. Import-Module, C:Program Files\Citrix\Provisioning Services\Citrix.ProvisioningServices.dll
   b. Get-Command-Module

The following image illustrates command options:

```
c. 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.

```
d. Login 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 username> -Password <PVS Admin
    password>

**Use Pass-in P SCredent ial object:**

```



```
9  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 blacklist.
- **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:**
>
> The rest of the PowerShell cmdlets are all part of the DatabaseAccess 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 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, rather 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 should address the needs of most AD environments, resulting in faster Configuration Wizard and Console
operations.

Modifying the search approach

For some special AD environments, typically 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, a
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.

CIS Problem Reporting

August 30, 2018

Citrix Provisioning allows you to report problems you encounter while using the software. Using this feature, you can directly report issues to Citrix Support, who uses the information to troubleshoot and diagnose the problem to improve Citrix Provisioning. This feature, along with the Customer Experience Improvement Program (CEIP), is used by Citrix to continually improve the software.

> **Note:**
>
> Participation in programs that help improve Citrix Provisioning is voluntary. Problem reporting, along with CEIP, are enabled by default. Use the information in this article to configure and use problem reporting.

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 Provisioning Server, or for a site:

- If you have an environment with multiple Provisioning Servers, each may have 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 will generate 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.
- The diagnostic bundle can be uploaded directly to Citrix, or it can be saved to a shared network drive and manually uploaded to Citrix at a later time.

> **Note:**
>
> The diagnostic bundle is manually uploaded to the Citrix CIS website; login to this site using your Citrix credentials.

Using a token for secure communication

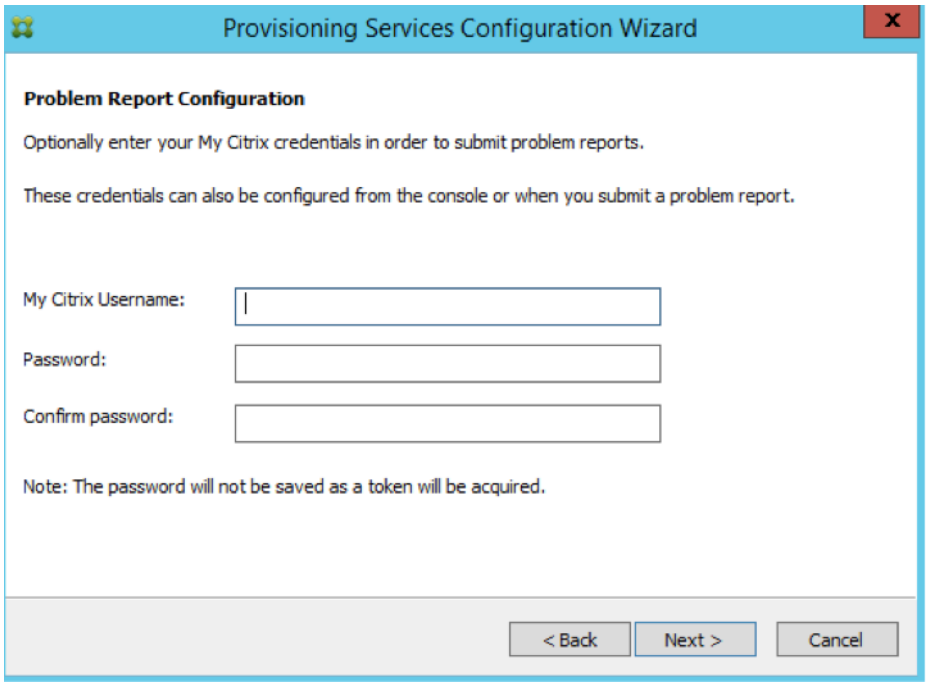
When using problem reporting, a token is generated to associate the diagnostic bundle with your My Citrix account login credentials. Once the token is associated with your My Citrix credentials, it is stored in the database for all future problem reporting, thus eliminating the need to store your login credentials.

> **Note:**
>
> If you are using Problem Reporting for the first time and have not yet configured a login token, you will be prompted to enter your My Citrix login credentials. Once you enter your login credentials, the token will be generated and stored in the database.

Configure problem reporting

In the Citrix Provisioning Configuration Wizard screen:

1. Enter your Citrix username and password.
2. Confirm the password.
3. Click **Next**.



> **Tip:**
>
> If you haven not secured a token used to authenticate your login credentials, the **Problem Report Configuration** screen displays information indicating that 'The token required to submit problem reports is empty. Please re-configure.' The token can be generated by entering your credentials here or at a later time using the Provisioning Console.
>
> You are prompted to enter your My Citrix credentials when you try to upload a problem report, and you have not yet generated the token.

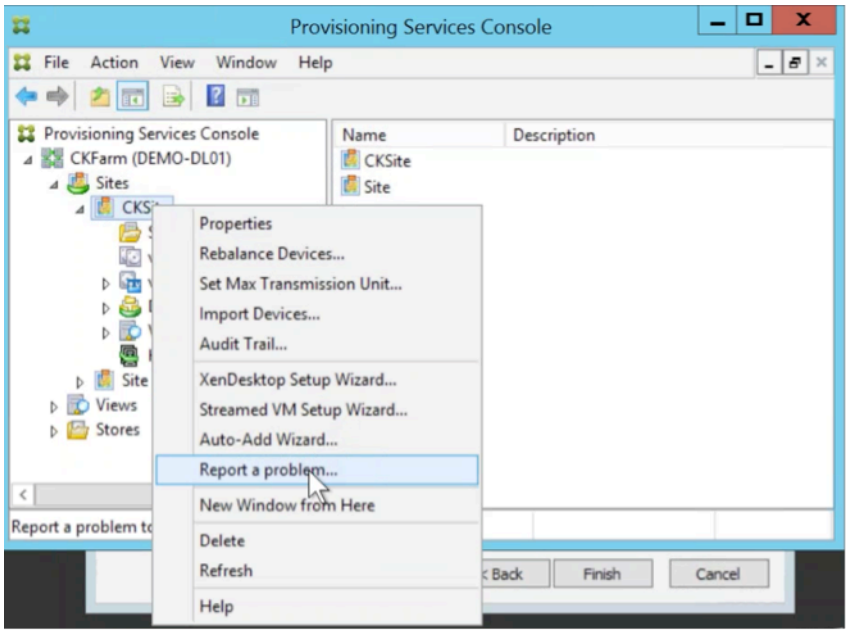
The password and username you specify are not saved. The token that is generated is used to associate your diagnostics bundle with your My Citrix account.

Report a problem

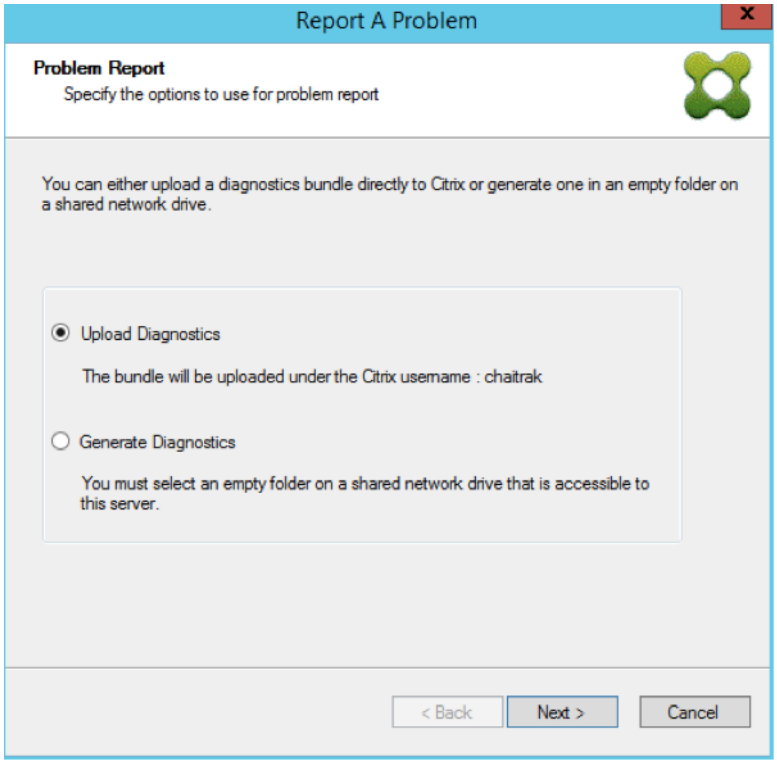
To report a problem you must first specify the options to use. You can either upload a bundle of diagnostic information using your Citrix username, or you can generate diagnostic information locally to a ZIP file by selecting an empty folder on a shared network drive accessible to all of the servers included in this 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. Select the server, and right click to display a context menu.
3. Click the **Report a problem** option.



4. In the **Problem Report** screen, select how to generate diagnostic information:
   - **Upload Diagnostics** – Use the generated token to upload a diagnostic bundle (a ZIP file containing numerous files related to the problem).
   - **Generate Diagnostics** – Select an empty folder on a shared network drive that is accessible to the servers you have selected.
5. Click **Next**.



> **Note:**
>
> Each server in the selected site uploads or generates its own diagnostic bundle.
>
> The token is only required for automatic upload. If you are generating the bundle locally, the token is not required.

6. After selecting the method to report a problem, you can 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.

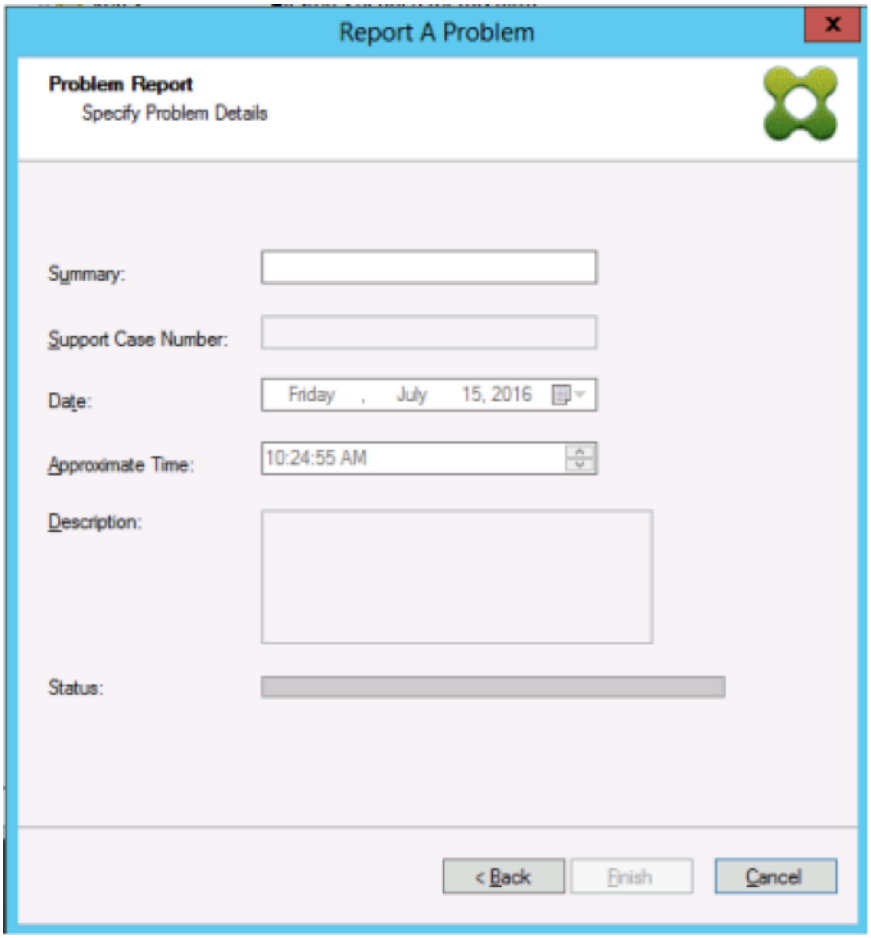
   b. Optionally enter a support case number.

   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.

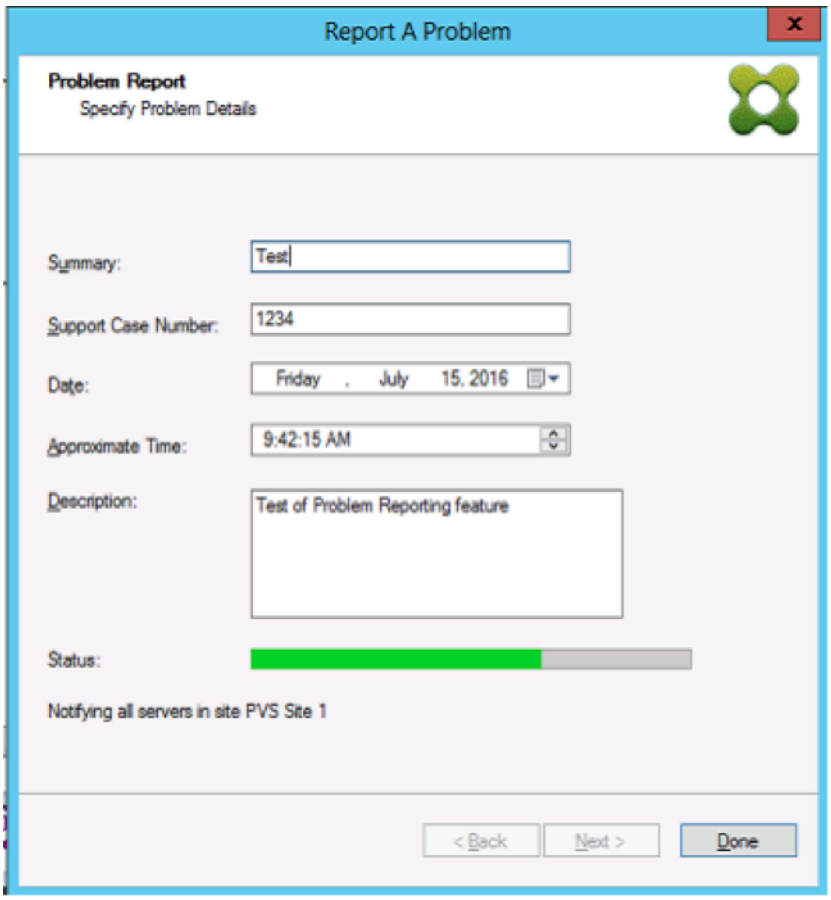
7. Click **Finish**.



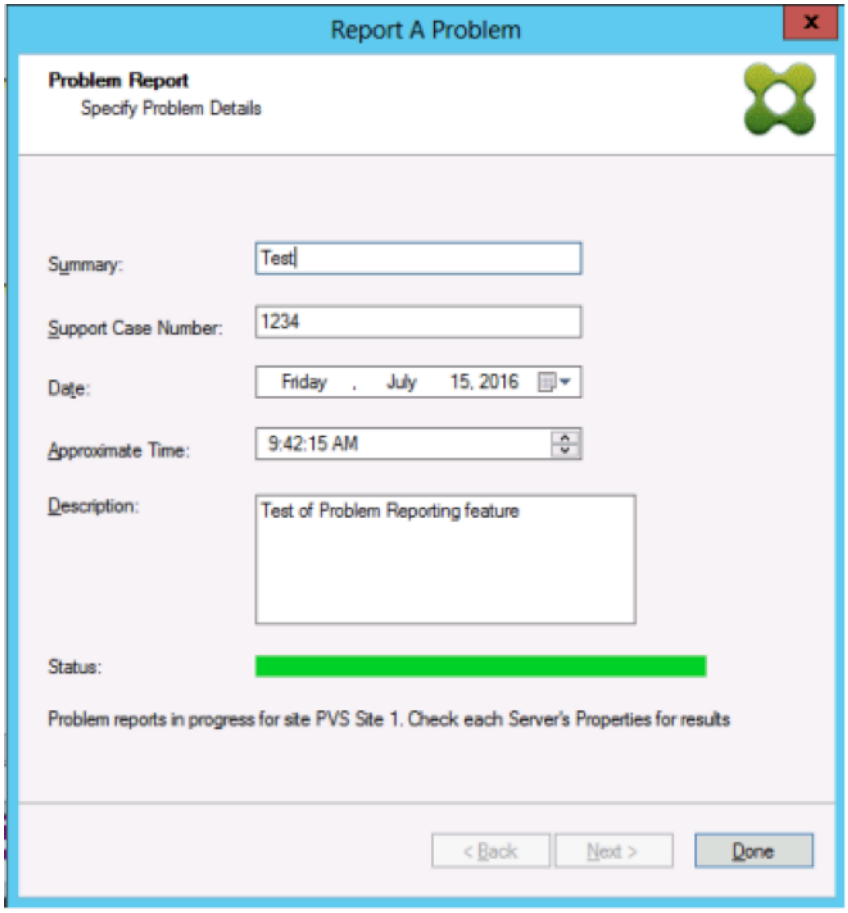
> **Tip:**
>
> After finishing, the bundle is created on the server(s) and uploaded. You can view the status of the most recent problem report from Server>Property>Problem Report.

After clicking **Finish**, the problem reporting function reports the issue for either a single server, or for each server in an entire site. Each server generates the problem report as a background task and uploads it to the CIS server (or, alternately, saves the file to a shared network drive).

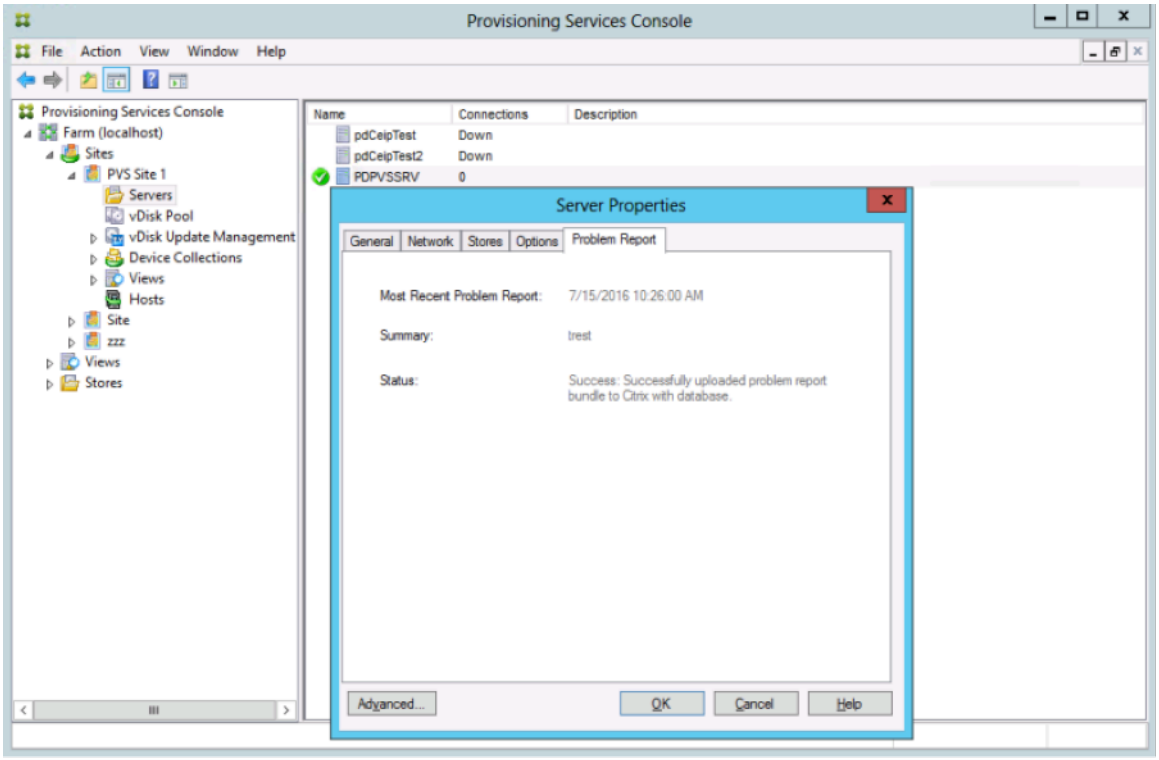
The **Status** field displays information indicating the state of the reporting mechanism; once the process starts, use the **Done** button to dismiss the dialog to allow the process to continue in the background:



If you choose not to dismiss the dialog, the process continues in the foreground; once completed, the Problem Report screen provides additional information stating “Check each Server’s Properties for results.” With this message, each server has completed the problem report generation process and saves the results (report generation success or failure).



Once the problem report is generated, you can view the results in 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 report attempt.
- **Summary**. This field describes the problem; it's 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 uploaded or saved to a shared network drive; if the report was saved to a drive, the full path where the file is located is displayed.

