Provisioning Services 7.15

Contents

What's new

July 29, 2022

This release of Provisioning Services provides expanded platform support for Linux Streaming on Ubuntu desktop 16.04. It also allows provisioning to Nutanix Acropolis hypervisors. See the fixed and known issues for additional information about this release of Provisioning Services.

Available as of July 29, 2022, Cumulative Update 9 adds fixes for customer-reported issues.

> **Note**
>
> Use the most recent version of the Citrix License Server to get the latest features. If you are upgrading from an existing version of Provisioning Services to the newest version of Provisioning Services, 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.

Fixed issues

August 26, 2022

Provisioning Services 7.15 CU9 (7.15.45)

Server

- Removing or marking down two vDisks in the Citrix Provisioning Console fails, with an error message **A database error occurred**. This error condition appears when you convert a character string to an unique identifier. [CVADHELP-18484]
- The stream process stalls. This issue occurs in environments where the SNMP server randomly sends a request packet, containing no data, to stream process ports. [CVADHELP-18600]

Provisioning Services 7.15 CU8 (7.15.39)

Server

- The TFTP service configured on a Provisioning Server might consume high memory. [CVADHELP-15299]

- With this fix, you can install Citrix Provisioning target devices by using Microsoft System Center Configuration Manager (SCCM). [CVADHELP-15749]
- The stream process (StreamProcess.exe) might fail to recover from hung threads. [CVADHELP-15775]
- With this fix, Citrix Provisioning adds NVMe controller support for target devices using ESX. The presence of the controller is determined on the Citrix Virtual Apps and Desktops Setup Wizard template. It is used when creating the write cache disk and the BDM disk. For BDM Update scenarios, Citrix Provisioning determines whether the controller exists on the provisioned VM and then updates the disk using the controller. [CVADHELP-15788]
- The Citrix Provisioning virtual disk might be forced to reconnect intermittently by the server. [CVADHELP-16457]
- After upgrading Citrix Provisioning Services from version 7.15 LTSR to version 1912 LTSR CU2, the available network interfaces might be missing from the TFTP configuration tool (Tftpcpl.cpl). [CVADHELP-16888]
- Attempts to merge the vDisk versions to a base image might fail causing this error message to appear:

  The parameter is incorrect. Error number 0xE00000057.

  [CVADHELP-16921]

Target Device

- The imaging wizard and P2pvs cannot fully image UEFI windows if the partition layout is customized. [CVADHELP-14553]
- The PVS Device Service (BNDevice.exe) might consume a high percentage of CPU usage. [CVADHELP-14870]
- When you configure UEFI PXE with DHCP Option 17 through a custom port, a target device might fail to start. [CVADHELP-16036]

Provisioning Services 7.15 CU7 (7.15.33)

Console

- Attempts to create virtual machines using the XenDesktop setup wizard might fail. [CVADHELP-13752]
- In the Citrix Provisioning console, attempts to copy and paste target device properties by using a mouse might fail. [CVADHELP-15568]

Server

- In a multi-homed PVS server environment, attempts to download the tsbbdm.bin file might fail. [CVADHELP-13948]
- Debug logs associated with target devices are not included in Always-on Tracing (AOT) or CDF traces sent to the Citrix Provisioning server. [CVADHELP-14829]
- You cannot view the **Farm is already configured** option when you run the Configuration wizard. The issue occurs after you upgrade Provisioning Services. [CVADHELP-14860]
- Attempts to open the Provisioning Services Console after restarting the Provisioning Server might fail with this error message:

  An unexpected MAPI error occurred

  [CVADHELP-15141]
- Target devices cannot start correctly and as a result keep on restarting. [CVADHELP-15144]
- When you configure the **Streamprocess** parameters using the **StreamProcess.cfg** file, the stream process (StreamProcess.exe) might fail to start. [CVADHELP-15295]
- The TFTP service in the Provisioning server consumes large amounts of RAM. [CVADHELP-15299]
- VDAs fail to start in scenarios where DNS name resolution and BDM are used with Infoblox DNS and DHCP. [CVADHELP-15724]
- With this fix, you can install Citrix Provisioning target devices by using Microsoft System Center Configuration Manager (SCCM). [CVADHELP-15749]
- With this fix, Citrix Provisioning adds NVMe controller support for target devices using ESX. The presence of the controller is determined on the Citrix Virtual Apps and Desktops Setup Wizard template. It is used when creating the write cache disk and the BDM disk. For BDM Update scenarios, Citrix Provisioning determines whether the controller exists on the provisioned VM and then updates the disk using the controller. [CVADHELP-15788]
- Changes to scheduled updates you make through vDisk Update Management do not take effect until you restart the Citrix PVS Soap Server service. [CVADHELP-16410]

Target Device

- The imaging wizard and P2pvs cannot fully image UEFI windows if the partition layout is customized. [CVADHELP-14553]
- The PVS Device Service (BNDevice.exe) might consume a high percentage of CPU usage. [CVADHELP-14870]

- With this fix, Citrix Provisioning target devices can be installed using Microsoft System Center Configuration Manager (SCCM). [CVADHELP-15590]
- With this fix, you can install Citrix Provisioning target devices by using Microsoft System Center Configuration Manager (SCCM). [CVADHELP-15749]

Provisioning Services 7.15 CU6 (7.15.27)

Console

- Permission problems associated with site administrator and device administrator roles. [CVADHELP-13302]
- In the Citrix Provisioning console, attempts to copy and paste the target device properties by using a mouse might fail. [CVADHELP-13361]
- The XenDesktop setup wizard might fail with an error when the Microsoft SCVMM server and the Hyper-V cluster are present on different domains. [CVADHELP-13762]

Server

- Target devices might become unresponsive on XenServer. The issue occurs when the CPU usage is high. [CVADHELP-11365]
- Registry hive file in the virtual disk version (AVHD) was corrupted when KMS restore was performed as a remote operation. [CVADHELP-12690]
- Permission problems associated with site administrator and device administrator roles. [CVADHELP-13302]
- When you use a PowerShell command to create a bootable ISO file (boot.iso), the option to set the network interface index might not be present in the BDM PowershellSDK. [CVADHELP-14362]
- Adding a machine resource using Studio results in an error message indicating that the provisioning server cannot connect to the specified port number. [CVADHELP-13348]

Target Device

- Registry hive file in the virtual disk version (AVHD) was corrupted when KMS restore was performed as a remote operation. [CVADHELP-12690]

Provisioning Services 7.15 CU5 (7.15.21)

Console

- The UEFI devices that are configured for BDM are unable to use a non-default custom network port range. [LD0706]
- Citrix Virtual Apps and Desktops setup wizard fails on GEN2 target devices when `useTemplateCache` is enabled. [LD0900]
- The `LimitCPUForMigration` template setting is ignored. [LD1071]
- When streaming target devices with Generation 2 virtual machines, Provisioning Servers might not be load balanced correctly. [LD1241]
- Attempts to access the farm from the console might fail. The issue occurs when the user is a member of the provisioning administrative group in a domain that is different from the user's domain. [LD1371]

Server

- Attempts to access the farm from the console might fail. The issue occurs when the user is a member of the provisioning administrative group in a domain that is different from the user's domain. [LD1371]
- Merging virtual disk versions that reside on the Resilient File System (ReFS) might take a long time on Windows Server 2016. [LD1783]
- The Configuration wizard might fail to complete when the SQL mode1DB is greater than the default database. [LD1957]
- The stream process (StreamProcess.exe) might exit unexpectedly when you switch the database from offline to online. [LD1958]

Target Device

- Some target devices repeat the Citrix Provisioning reconnect login process after SQL server failover. [LD1822]

Provisioning Services 7.15 CU4 (7.15.15)

Console

- The System Center Virtual Machine Manager (VMM) was set up to manage multiple top level host groups. If you run the Citrix Virtual Apps and Desktops Setup Wizard and connect to a Hyper-V environment, this error message might appear:

Cannot connect to the hypervisor - An item with the same key has already been added. [LD0047]

- With this fix, the **New-PvsSite** command might not contain -VirtualHostingPoolId, -VirtualHostingPoolName, and -XsPvsSiteUuid as mandatory parameters. [LD1209]

Server

- When an additional virtual hard disk (VHD) footer is assigned to a merged VHD, the file size of the merged base might increase. [LC9837]
- The BNTFTP.exe process might exit unexpectedly. The issue occurs when there is a security check failure or a stack buffer overrun. [LD0250]
- A Citrix Provisioning server installed on Windows Server 2012 and earlier might experience issues when merging an existing virtual disk version to a new merged base on a virtual disk with VHDX format. This issue occurs when a virtual disk is stored on a Resilient File System (ReFS) on a Windows Server 2016 or newer and accessed over Server Message Block (SMB). Merging virtual disk versions to a new merged base fails. The following error message might appear:

  The parameter is incorrect. Error number 0xE00000057. [LD0437]
- After upgrading Provisioning Services from Version 7.6 CU2 to Version 7.15 CU2, the target device might experience a fatal exception and display a blue screen. The issue occurs due to null pointer pointing to a personality string. [LD0546]
- The UEFI devices that are configured for BDM are unable to use a non-default custom network port range. [LD0706]

Target Device

- The **Enable auto update controller** policy might fail to take effect on a Citrix Provisioning Windows target VDA. The issue is due to the lack of network service permission, causing the Broker Agent service's failure to access **SavedListOfDdcsSids.xml** in the persistent data location (d:\pvsvm). [LD0450]

Provisioning Services 7.15 CU3 (7.15.9)

Console Issues

- The XenDesktop Setup Wizard might attempt to connect to an incorrect Hyper-V Host. The issue occurs when there are multiple clusters managed by the same System Center Virtual Machine

Manager (SCVMM) server. [LC8415]

- The Boot Device Manager (BDM) might fail to update on the XenServer that is created on the slave XenServer. [LC8964]
- The Provisioning Services audit trail might show an incorrect text description for some entries. The data saved in the database for the entries is correct, but the description shown in the audit trail window is incorrect. [LC9481]
- The Provisioning Services XIP library for VMware ESXi does not support TLS v1.2. [LC9629]
- When you upgrade the Provisioning Services Server or the Console software, the PowerShell snap-ins might not be upgraded. [LC9718]
- The Provisioning Server Unified Extensible Firmware Interface (UEFI) bootstrap might not accept boot menu input if there are multiple vDisk versions to choose from. The keyboard input becomes unresponsive during the PXE or BDM boot process of a physical target device that is booting in Maintenance mode. [LC9815]
- When using the XenDesktop Setup Wizard, attempts to create the Boot Device Manager (BDM) partition fails when using the VMware ESX vSAN configuration. [LD0029]

Server issues

- After promoting a vDisk to production, the vDisk might remain mounted on the Provisioning Services Server. [LC8051]
- KMS handling is not applied to vDisk versions. [LC8147]
- The same disk identifier is erroneously assigned to the vDisk residing in different stores when the existing vDisk was added using the "MCLI Add DiskLocator"command. [LC8281]
- Provisioning Services fails to mount a vDisk when the VHDX size is 512 MB and the physical storage size is 4,096 MB. [LC8430]
- When applying Microsoft Hotfix KB3186539 on servers running Japanese and Chinese versions of Windows, the Boot Device Manager (BDM) platform cannot be created. [LC8743]
- The Boot Device Manager (BDM) might fail to update on the XenServer that is created on the slave XenServer. [LC8964]
- When you merge two or more vDisks at the same time, the MgmtDaemon.exe process might exit unexpectedly. [LC9123]
- When you create a merged base vDisk version, the MgmtDaemon.exe process might exit unexpectedly with an exception code 0xc0000005. [LC9143]

- The Provisioning Services audit trail might show an incorrect text description for some entries. The data saved in the database for the entries is correct, but the description shown in the audit trail window is incorrect. [LC9481]
- After upgrading XenApp and XenDesktop from Version 7.13 to Version 7.15, local users might not be able to log on to the Provisioning Services Console. A timeout error message appears. [LC9542]
- The Provisioning Services XIP library for VMware ESXi does not support TLS v1.2. [LC9629]
- When you upgrade the Provisioning Services Server or the Console software, the PowerShell snap-ins might not be upgraded. [LC9718]
- On Provisioning Services 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 PVS is installed in a Workgroup environment. [LC9844]
- When using the XenDesktop Setup Wizard, attempts to create the Boot Device Manager (BDM) partition fails when using the VMware ESX vSAN configuration. [LD0029]
- After you upgrade Provisioning Services from Version 7.6.x to 7.15 LTSR CU2 and attempt to open the **Provisioning Services Console**, this error message might appear:

  An unexpected MAPI error occurred [LD0092]

Target device issues

- Attempts to install a PVS Linux Target device might fail. The issue occurs when the required dependencies on Ubuntu are incorrect. [LC9478]

Provisioning Services 7.15 CU2 (7.15.3)

Console Issues

- When using a Provisioning Server with the Finnish locale installed, attempts to create virtual machines using the XenDesktop Setup Wizard might fail and the following error message appears:

  "The bdmCreated field is not formatted properly, the correct format is YYYY-MM-DD HH:MM." [LC7866]

Server issues

- When using a Provisioning Server with the Finnish locale installed, attempts to create virtual machines using the XenDesktop Setup Wizard might fail and the following error message appears:

"The bdmCreated field is not formatted properly, the correct format is YYYY-MM-DD HH:MM." [LC7866]

- When the Boot Device Manager (BDM) is configured for the DHCP Discover, Offer, Request, and Acknowledge (DORA) process, the process might not complete. The issue occurs when the DHCP relay sends the "OFFER"packet as a UNICAST packet. [LC8130]
- The trust relationship of the Linux target device might be lost with Active Directory, when the machine account password for the target device expires. [LC8331]
- Target devices cannot start correctly and as a result keep on restarting. [LC8358]
- A target device that is part of a Delivery Group fails to boot after upgrading from a previous PVS version. [LC8378]
- The XenDesktop Setup Wizard might attempt to connect to an incorrect Hyper-V Host. The issue occurs when there are multiple clusters managed by the same System Center Virtual Machine Manager (SCVMM) server. [LC8415]
- The response of the configuration wizard and Provisioning Services Console operations might be slow or the Console might time out in an Active Directory environment. [LC8692]
- Target devices might randomly stop communicating with the Provisioning Server during the initial read operation from the personal vDisk (single I/O stage). [LC8745]
- When you attempt to copy and paste the vDisk properties between two vDisks, the properties might not be pasted on the second vDisk. [LC8767]
- This enhancement is a backport of functionality introduced in Provisioning Services 7.17. It is included in response to customer requests. For more information, see Enhanced multi-tier Active Directory group search. [LC9064]
- This enhancement is a backport of functionality introduced in Provisioning Services 7.17. It is included in response to customer requests. For more information, see Enhanced multi-tier Active Directory group search. [LC9066]
- The Stream Service might exit unexpectedly while the Provisioning Server appears to be down in the Servers node. [LC9138]

Target device issues

- Target devices might become unresponsive. [LC7911]
- A Unified Extensible Firmware Interface (UEFI) target device might experience a fatal exception, displaying a blue screen, on CVhdMp.sys with stop code 0x0000007E. This exception might occur when you start a UEFI target device from a vDisk configured with NIC teaming. [LC8548]

- Target devices might become unresponsive. [LC8897]
- Microsoft Windows 10 v1709 might experience a fatal exception, displaying a blue screen when present in private mode. [LC8979]
- Microsoft Windows 10 v1709, 32 bit cannot start from a vDisk in private image mode. [LC8980]
- Target devices that are running on Microsoft Windows 10 might become unresponsive at the Getting devices ready screen while restarting. [LC8844]
- Target devices might become unresponsive at the Windows logo or the splash screen. [LC9104]

Provisioning Services 7.15 CU1 (7.15.1)

Console Issues

- The XenDesktop Setup wizard might fail after creating a template virtual machine. [LC8018]

Server issues

- In a network environment where the MTU size is less than 1,500 bytes, the bootstrap file fails to download. Target devices fail to start using the Boot Device Manager (BDM). This enhancement allows you to lower the MTU size to less than 1,500 bytes by setting the following registry key. The enhancement is disabled by default:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\PVSTSB\Parameters
  Name: MtuSize
  Type: DWORD
  Value: MTU size you want to configure in decimal. If the value is below 512, 512 bytes is used. If the value is larger than 1,500, 1,500 bytes (default) is used. The fix is disabled by default. If the value is set to 0, the fix is also disabled. [LC8474]

Provisioning Services 7.15

Console Issues

- Editing the partition size using the imaging wizard does not work in PVS 7.1x. [LC7967]

  The following Nutanix issues have been resolved in this release:

- After provisioning an Acropolis hypervisor using the XenDesktop Setup Wizard, you cannot start the hosted machine using **Boot Device…** from the PVS Console.
- PVS targets do not support Cache on Server and Cache in device RAM.

Server issues

- Server communication time-out. Sometimes, login times can become excessively long (for example, greater than 2 minutes). This lapse can cause server timeout issues between the PVS Console and the Soap Server. By default, the timeout for such connections is 2 minutes. However, you can increase this value by modifying the registry value HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=<timeout in seconds>. If the login time is greater than approximately 4 minutes, users experience timeouts from the Microsoft MMC containing the PVS Console (these timeouts can be dismissed).

  One cause for this issue is unreachable domains in Active Directory. There is a 30 second timeout applied each time an attempt to connect to an unreachable domain is made. These connection attempts can quickly add up to several minutes if there are multiple unreachable domains. In general, unreachable domains are created by adding a test or experimental domain to Active Directory, then removing it later. Although the domain is gone, it is still reported by Active Directory when enumerating domains or authorization groups.

  Unreachable domains are caused by a domain controller being temporarily shut down and disconnected from the network, so not all unreachable domains should be blacklisted.

  The best way to determine whether there are unreachable domains is by looking at the CDF trace for the PVS_DLL_ADSUPPORT module. Check these traces for "Unreachable Domain"and "Server Referral"errors. If any of these are found, check the domains to ensure that they are not in use any more, and if not, add the domain names to the blacklist.

  The blacklist is a JSON format file called "%ProgramData\Citrix\Provisioning Services\blacklist.json" . For example:

  ```
  {
  "Domains":
  [
  "sub.xs.local,"
  "sb.xs.local"
  ]
  }
  ```

  where the two domains **sub.xs.local** and **sb.xs.local** are excluded from domain and group enumeration. After the file is updated, you must restart the Soap Server and any running consoles to load the updated values. [LC6249]

- Soap service crashes when adding a new store using the console. [LC8165]

Known issues

January 4, 2019

- 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.
- Provisioning Services supports Windows 10 Fall Creator v1709 with the following known issues:
  - Target device uninstallation hangs on Windows 10 v1709. To resolve this issue, use the in-place upgrade for the target device. [LCM-3219]
  - Windows 10 32 bit v1709 cannot boot from a vDisk in private image mode. [LCM-3224]
- When using the PVS 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 configuration 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]

- When creating a vDisk on Ubuntu (version 16.04.2), error messages appear at the beginning and ending of the process. Click **OK** to continue with the successful creation of the vDisk. This issue does not affect image creation.

[#PVS-2200]

- When using the Linux streaming feature in some localized environments (for example, Japanese) wrong characters appear when using the configuration image wizard.

[#PVS-1454]

- Uninstall fails after a target device is upgraded using the Windows 10 Fall Creator update. Provisioning Services does not support Windows 10 Fall Creator (v1709). However, it does support the latest semi-annual Windows 10 release at the time that version was made available.

[#PVS-3123]

- Unable to create a machine catalog with an on-premises PVS server. This occurs when you try to create a PVS machine catalog from Studio when a PVS machine (from the on-premises PVS server) does not have an AD account associated with it. To resolve the issue, when creating a PVS machine catalog using Citrix Cloud Studio and DDC:

1. Connect to an on-premises PVS server.

2. Select a PVS collection.
3. Import the machines from that collection into a XenDesktop machine catalog. **Note**: The PVS machines must have AD accounts associated with them.

[#XACO-674]

- The following Nutanix issues exist at this release:
  - You cannot import an existing PVS collection when using XenDesktop or Studio.
  - When provisioning an Acropolis hypervisor using the XenDesktop Setup Wizard, select a snapshot without a hard disk selected to ensure that the snapshot becomes the new VM.
  - The XenDesktop Setup Wizard reports misleading error messages when invalid credentials are specified while connecting to an Acropolis hypervisor. This issue is consistent with other hypervisor platform error conditions that use invalid credentials.
  - A Nutanix Acropolis hypervisor does not support AVU (automatic vDisk update). [#PVS-2164]

Deprecation

October 23, 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 Provisioning Services version that is part of the next XenApp and XenDesktop Long Term Service Release (LTSR). Deprecated items will be removed in a Current Release following the next LTSR. Alternatives for deprecated items are suggested where possible.

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

Item	Announced in	Alternative
Printer management (labeled **Enable printer management**) in the vDisk Properties screen.	7.12	

Item	Announced in	Alternative
In the BDM Media Properties section of the Boot Device Management screen, the term **BDM Secure Boot**.	7.12	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. **Note**: The cache on hard disk parameter will be removed due to lack of ASLR support.	7.12	Use one of the other available options.

System requirements

December 8, 2021

Introduction

The system requirements in this article were valid when this product 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 Provisioning Services.

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 2012 through 2016 (x86, x64, and Express editions).

Database clustering is supported.

When configuring databases for provisioning, consider that no preference exists for any specific SQL collation. Collation supports the standard method recommended by Citrix Virtual Apps and Desktops when using the configuration wizard. The administrator creates the database with a collation that ends with `_CI_AS_KS`. Citrix recommends using a collation that ends with `_100_CI_AS_KS`.

> **Note:**
>
> Refer to Supported Databases for XenApp and XenDesktop 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 XenApp/XenDesktop installation media. You should always use the most recent Citrix License server to get the latest features.

> **Important:**
>
> 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 PVS to avoid any licensing conflicts related to grace periods. For more information, see Licensing.

Provisioning Server

Operating systems

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

English, Japanese, and Simplified Chinese versions are supported.

Processors

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. Your streaming performance can be improved 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.

PVS dependencies

The Provisioning Server install program requires Microsoft NET 4.6.1 and Windows PowerShell 3.0.

Network

UDP and TCP ports

Provisioning Server to Provisioning Server communication

- Each Provisioning Server must be configured to use the same ports (UDP) to communicate with each other using the Messaging Manager. At least five ports must exist in the port range selected. The port range is configured on the Stream Services dialog when the Configuration wizard is run.

  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

Target device to Provisioning Server communication

- Each Provisioning Server must be configured to use the same ports (UDP) to communicate with target devices using the StreamProcess.
- The port range is configured using the Console's Network tab on the Server Properties dialog.

Note: The first 3 ports are reserved for Provisioning Services.

Default port range (UDP) 6910–6930

Target device to Provisioning Services communication

Unlike Provisioning Servers to target device port numbers, target device to Provisioning Server 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\BNTFTP\Parameters Port

Default port (TFTP) 69

TSB

The TSB port value is stored in the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PVSTSB\Parameters Port

Default port (UDP) 6969

Port Fast

Port Fast must be enabled

Network card

PXE 0.99j, PXE 2.1 or later

Addressing

DHCP

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.

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, install and configure the OEM NIC teaming software
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 that runs on the device.

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

The operating systems identified below are supported for target devices:

Operating System

- Windows 10 (32-bit or 64-bit); all editions

> **Note:**
>
> Support for the publicly available version at the time of the release. For more information, see Windows 10 Compatibility with Citrix Virtual Desktops (XenDesktop).

- Windows 8 (32-bit or 64-bit) and Windows 8.1 (32-bit or 64-bit); all editions
- Windows 7 SP1 (32-bit or 64-bit); Enterprise, Professional, Ultimate.

Note: The Ultimate edition of Windows 7 is supported only in Private Image mode.

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

Gen 2 VMs

For Provisioning Services support of Gen 2 VMs in a XenDesktop environment, the following operating systems are supported:

- Windows 2016, Windows 10 (with or without secure boot)

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

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

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)

> Note:
>
> When using these distributions for Linux streaming, consider that the PVS installer requires that the Linux kernel package version be greater than or equal to version 4.4.0.53. The PVS installer automatically provides the correct version during the installation process.

- RedHat Enterprise Linux Server 7.2
- CentOS 7.2
- SUSE Linux Enterprise Server (SLES) 12.1, 12.2

Note: The default kernel used for Ubuntu 16.04.2 is version 4.8; this kernel version is not currently supported.

Additional dependencies

.NET 4.6.1

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, and Windows Server 2012 are deployed using either 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.

Note: 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**
>
> Provisioning Services English on English, Japanese, German, French, Spanish, Simplified Chinese, Traditional Chinese, Korean, and Russian versions of operating systems are supported.

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; Standard, Essential, and Datacenter editions
- Windows Server 2012 R2; Standard, Essential, and Datacenter editions
- Windows 10 (32-bit or 64-bit)
- Windows 8.1 (32-bit or 64-bit); all editions
- Windows 8 (32-bit or 64-bit); all editions
- Windows 7 (32-bit or 64-bit)

Additional dependencies

MMC 3.0, Microsoft .NET 4.5.2, Windows PowerShell 3.0

Store

The store must be able to communicate with the Provisioning Services database.

XenDesktop Setup Wizard

The Provisioning Services XenDesktop Setup wizard operates only with the equivalent version of the XenDesktop controller, that is, the version levels must be the same. In addition:

- One or more configured XenDesktop hosts with identical templates must exist.
- A Device Collection must have been created in the Provisioning Services Site.
- The vDisk that will be assigned to each VM must be in standard image mode.

Additional requirements include:

Permissions

- A XenDesktop controller must exist with permissions for the current user.
- vCenter, SCVMM, and XenServer minimum permissions must be configured.
- A Provisioning Services Console user account must be configured as a XenDesktop administrator and must have been added to a PVS SiteAdmin group or higher.
- If you are using Provisioning Services with XenDesktop, the SOAP Server user account must have XenDesktop 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 XenDesktop, 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 XenDesktop catalog using the XenDesktop Console. See the XenDesktop 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 as follows:

  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 Active Directory Users and Computers MMC when exporting the contents of an organizational unit.

- If you are using Personal vDisks with XenDesktop, the SOAP Server user account must have XenDesktop full administrator privileges.

SCVMM

- SCVMM servers require that PowerShell 2.0 is installed and configured for the number of 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 XenDesktop, the user must run the following PowerShell command;set-ExecutionPolicy unrestricted on SCVMM.
- For Microsoft SCVMM, please 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 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\ProvisioningServices\PlatformEsx
  - Create a new string in the PlatformEsx key named ServerConnectionString and set it to `http://{ 0 } :PORT\\#/sdk`

    > **Note:**
    >
    > If using port 300, `ServerConnectionString= http://{ 0 } :300/sdk`

- If using multiple NICs, the XenDesktop wizard assumes that the first NIC is the Provisioning Services 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 Provisioning Services XenDesktop Set Up Wizard is used with SCVMM, both the first legacy and the synthetic NICs'network will change according to the network resource set by XenDesktop, or by the user if SCVMM host has multiple network resources.
- Multi-NIC support for XenDesktop private virtual machine desktops.

- Legacy XenDesktop Virtual Desktop Agents are supported on VMs. For details, refer to VDA requirements in the XenDesktop 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 Provisioning Services Site.
- A vDisk in Standard Image mode must exist, to be associated with the selected VM template.

Addtional requirements are described in the table below:

Template VM

- Boot order: Network/PXE must be first in list (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 Provisioning Services Console user account must have been added to a PVS SiteAdmin group or above.
- If you are using Active Directory, 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.

ESD server requirements for vDisk Update Management

ESD server requirements are described in the table below:

WSUS server

3.0 SP2

SCCM

SSCM 2016

SCCM 2012 R2

SCCM 2012 SP1

SCCM 2012

Hypervisor

The following sections include configuration information about supported hypervisors.

> **Important:**
>
> Refer to Supported Hypervisors for Virtual Desktops (XenDesktop) and Provisioning Services for a complete list of supported hypervisors.

XenServer 5.6 and later

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

Nutanix Acropolis

This release provides support for provisioning to Nutanix Acropolis hypervisors using the XenDesktop Setup Wizard. The following are **not** supported:

- Linux VMs
- BDM partition
- UEFI

For configuration information, refer to Deploying virtual desktops to VMs using the XenDesktop Configuration Wizard.

> **Important**
>
> An Acropolis hypervisor (AHV) plugin from Nutanix that supports Provisioning Services is required.

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

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 Provisioning Services XenDesktop Set Up Wizard changes the vlan of both NICs to the vlan selected during the XenDesktop Set Up Wizard run. This uses two IP addresses
- When running the imaging wizard, make sure you select the legacy NIC's MAC address.
- Provisioning Services does not support multiple legacy NICs in the VMM's VM. This is because VMM uses the last legacy NIC and XenDesktop 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 XenDesktop Set Up Wizard, you may find that the targets are created but are not bootable with the error Device not found in PVS dB. 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 fix this, delete the NICs in the template. Make a legacy NIC 1 and synthetic NIC 2.

VMware vSphere ESX

- vSphere ESX 6.7 (7.15 LTSR CU3 and later)
- vSphere ESX 6.5
- vSphere ESX 6.0
- vSphere ESX 5.5
- vSphere ESX 5.0 and later –VMXNET3
- Sphere ESX 4.x –E1000

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.

PVS 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 with VMXNET NICs

- Windows 7 without service packs —Install Microsoft iSCSI hotfix http://support.microsoft.com/kb/2344941 and restart the VM before installing Provisioning Services target device software.
- Windows 7 with Service Pack 1 –Install Microsoft iSCSI hotfix http://support.microsoft.com/kb/2550978 and restart the VM before installing Provisioning Services target device software.

ESX

- For ESX 5.0 only, the Interrupt Safe Mode must be enabled on the Provisioning Services 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's CD/DVD drive's 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 XenDesktop 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 XenDesktop host will be that of the vCenter system. Do not enter the address used by the web client.

Linux streaming

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 Provisioning Services installer requires that the Linux kernel package version be 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
- CentOS 7.2
- 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.

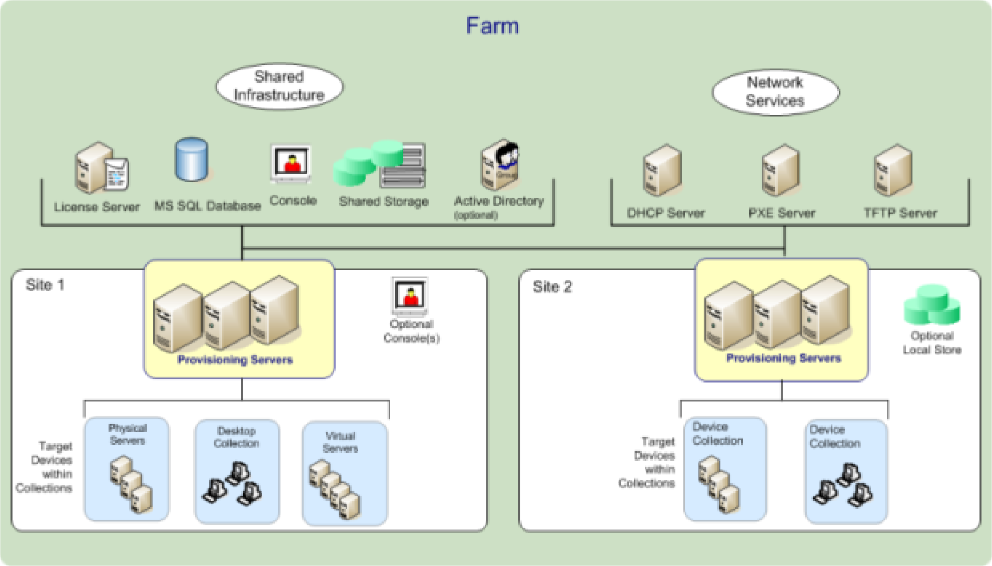
> **Important:**
>
> Linux streaming functionality works with the latest version of Provisioning Services in conjunction with corresponding versions of XenApp/XenDesktop.

Provisioning Services product infrastructure

May 28, 2019

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

The rest of the article provides a brief introduction to Provisioning Services components.



License Server

The product license server is installed within the shared infrastructure or you can use an existing Citrix license server.

> **Note**
>
> The license server is selected when the Configuration Wizard is run on a Provisioning Server. All Provisioning Servers within the farm must be able to communicate with the license server.

Provisioning Services 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 leverage 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 Provisioning Services 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.

> **Note**
>
> The Console is installed as a separate component and is available from the product installation media. The Provisioning Services Console is an MMC (Microsoft Management Console) snap-in. MMC specific console features are not described in this document. Refer to Microsoft's MMC documentation for detailed information.

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, and locate then 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 when the Configuration Wizard is run. Existing network services within your infrastructure can also be leveraged.

Farms

A farm represents the top level of a Provisioning Services infrastructure. The farm is created when the Configuration Wizard is run on the first Provisioning Server that will be 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.

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.

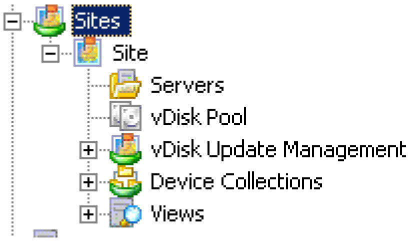
Store name (logical name): `financevdisks`

Physical path to the vDisk for all Provisioning Servers in the farm is: `\\\\\financeserver\\financevdisks\\`

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. Stream Services 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 Provisioning Services database. Provisioning Server configuration options are available to ensure high availability and load balancing of target device connections.

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.

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.

A target device can be a member of only one device collection.

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 Modes

vDisk images are configured to be in Private Image mode (for use by a single device, read/write) or Standard Image mode (for use by multiple devices, read-only with 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. The following illustrates the basic relationship between a base disk and versions that reference that base disk.

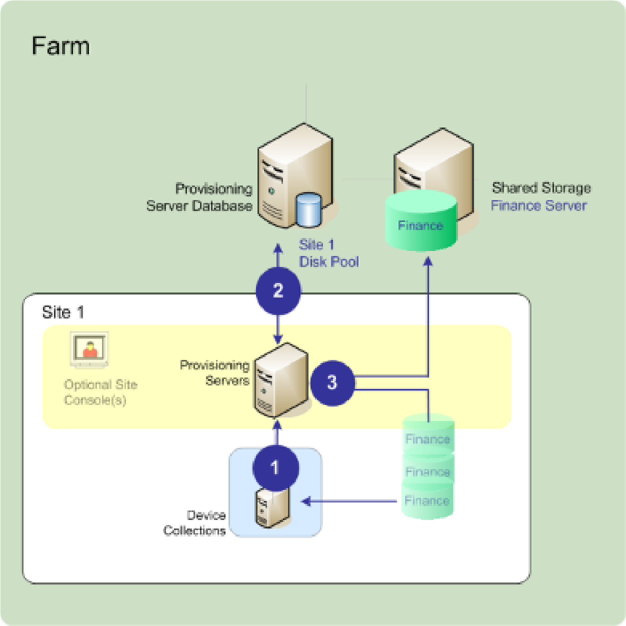
Each time a vDisk is to be updated, a new version of the VHDX differencing disk can be created and the file name is numerically incremented, as shown in the following table:

	VHDX Filename
Base Image	win7dev.avhdx
Version 1	win7dev.1.avhdx

	VHDX Filename
Version 2	win7dev.2.avhdx
…	…
Version N	win7dev.**N**.avhdx

Booting a vDisk

The method used to locate and boot from a vDisk on a server share is illustrated in the following graphic:

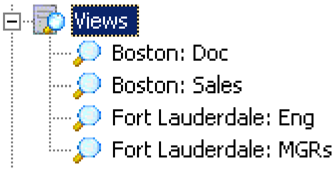


1. The target device begins the boot process by communicating with a Provisioning Server and acquiring a license.
2. The Provisioning Server checks the vDisk pool for vDisk information, which includes identifying the Provisioning Server(s) that can provide the vDisk to the target device and the path information that server should use 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.

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:



Views
Boston: Doc
Boston: Sales
Fort Lauderdale: Eng
Fort Lauderdale: MGRs

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

Provisioning Services administrator roles

May 28, 2019

The ability to view and manage objects within a Provisioning Services 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 share the same 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 dialog.

The following roles exist within a Provisioning Services farm:

- **Farm Administrator** –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.
- **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 can perform all device-collection management tasks on collections to which they have privileges, including view vDisk properties (read-only), assign or remove vDisks from a device, boot or shut down target devices, edit device properties, and send messages to target devices within a device collection to which they have privileges.

- **Device Operator** –Device operators can 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.

Product utilities

May 28, 2019

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

- Installation Wizard –Use this wizard to install Provisioning Services components to create a 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 Provisioning Services installation process.
- Imaging Wizard –On the master target device, run the Provisioning Services Imaging Wizard to create a vDisk file in the Provisioning Services database and then image to 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.
- XenDesktop Setup Wizard –Creates virtual machines (VMs) on a XenDesktop 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 XenDesktop 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 Provisioning Services.
- Upgrade Utilities –There are several upgrade methods available. The method you select depends on your network requirements.

- Programming Utilities –Provisioning Services provides programmers with a management application programming utility and a command line utility. These utilities can be 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.

Upgrading Provisioning Servers

November 4, 2020

In a Provisioning Services 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 may not be available. Citrix recommends closing all Consoles until the upgrade is complete to avoid failed operations.

> **Note**
>
> When upgrading from a CU release to another CU release (for example, from 7.15 CU1 to 7.15 CU2), you are not prompted to upgrade the database.

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 that will be used to manage the farm (for details on installing the Console, refer to Installing Provisioning Services Server Software.
3. In the Configuration Wizard (if the wizard does not start automatically after completing the product installation, start it now), 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 Configure the farm.

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.

> **Note**
>
> The database upgrade is ignored because the database was upgraded when the first server was upgraded.

Upgrading vDisks by reverse imaging

September 23, 2021

Upgrade by reimaging 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 reimaging upgrade method that you choose depends on your existing Provisioning Services 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 reimages 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 Services Consoles
- Creating a backup copy of the vDisk

To upgrade, complete the procedure that follows.

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 Provisioning Services Imaging Wizard to create a vDisk image, create the target device if it does not 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 PVS 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 Provisioning Services release to get the latest P2PVS.exe. The upgrade wizard can also be installed with the Provisioning Services meta-installer using the Target Device Installation > Install Upgrade Wizard option.
- Run P2PVS.exe from the Provisioning Services Upgrade Wizard directory (by default, this directory is C:\Program Files\Citrix\Provisioning Services Upgrade Wizard).
- Click the **From** drop-down menu and choose **Provisioning Services vDisk** and click **Next**.
- In the partition screen, select the partitions. All system partitions, regardless of whether they have a drive letter or not, are used in reverse imaging. Click **Next**.
- Click **Convert** on the last page to begin reverse imaging.

> **Important**
>
> Reverse imaging for BIOS systems is non-destructive. The partition table of the system is not altered. Because PVS 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 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 is lost as a result.

Automated inline upgrade

Use the Automated vDisk Upgrade method when upgrading from 5.1.x, 5.6.x, or 6.0–6.1, 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 Services 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 Auto Logon. This local account cannot have an empty password.
    b) Specify a local partition to which reverse imaging clones 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 Upgrade Manager. This account cannot have an empty password.
    d) Click **OK**.
    e) UpgradeConfig performs 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 reboots several times, and then display a message to indicate that the script has successfully completed.

> **Note**
>
> **Auto Logon** clears when the upgrade completes. If Auto Logon is wanted for vDisk deployment, setup Auto Logon 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 several modifications in Private Image mode
- The original hard drive is no longer available

The manual upgrade method includes completing the following tasks:

1. Image the 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 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, the Provisioning Server fails to connect with the vDisk.
9. Uninstall the product software.

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 at \Program Files\Citrix\Provisioning Services\P2PVS.exe.
8. 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.
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 fails to connect with the vDisk.
11. Uninstall the product software.

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 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.

> **Note:**
>
> This process applies to reverse imaging. For P2PVS processes Provisioning Services applies the deafult values automatically. Configuration changes only apply to situations where you want to

> image multiple disks or partitions.

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.

Pre-installation tasks

November 20, 2020

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

Select and configure the MS SQL database

Only one database is associated with a farm. You can install the Provisioning Services 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 Provisioning Services 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 Services software.

Database sizing

For information on database sizing, see Estimate the Size of a Database.

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:

- Database Version record requires approximately 32 KB
- Farm record requires approximately 8 KB
- Disk Create record requires approximately 16 KB

- Notifications require approximately 40 KB
- Server Mapped record requires approximately 16 KB

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

- Access and groupings (each)
    - A User group that has access to the system requires approximately 50 KB
    - A Site record requires approximately 4 KB
    - A Collection requires approximately 10 KB
- Farm View (each)
    - Farm View requires approximately 4 KB
    - FarmView/Device relationship requires approximately 5 KB
- Site View (each)
    - Site View requires approximately 4 KB
    - SiteView/Device relationship requires approximately 5 KB
- Target device (each)
    - A target device requires approximately 2 KB
    - Device Bootstrap requires approximately 10 KB
    - Device: Disk relationship requires approximately 35 KB
    - Device: Printer relationship requires approximately 1 KB
    - Device Personality requires approximately 1 KB
    - Device Status when a Device boot requires approximately 1 KB
    - DeviceCustomProperty requires approximately 2 KB
- Disk (each)
    - Unique disk requires approximately 1 KB
    - DiskVersion requires approximately 3 KB
    - Disk Locator requires approximately 10 KB
    - DiskLocatorCustomProperty requires approximately 2 KB
- Provisioning Server (each)
    - A server requires approximately 5 KB
    - ServerIP requires approximately 2 KB
    - Server Status when a Server boot requires approximately 1 KB
    - ServerCustomProperty requires approximately 2 KB
- Store (each)
    - Store requires approximately 8 KB

  - Store:Server relationship requires approximately 4 KB

- Disk update (each)

  - VirtualHostingPool requires approximately 4 KB
  - UpdateTask requires approximately 10 KB
  - DiskUpdateDevice requires approximately 2 KB
  - Each DiskUpdateDevice:Disk relationship requires approximately 35 KB
  - Disk:UpdateTask relationship requires approximately 1 KB

The following changes cause the size requirements to increase:

- Each processed task (for example: vDisk versionings 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 Provisioning Services 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 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 Provisioning Services Configuration wizard. No additional steps are required because the wizard considers the cluster as a single SQL Server.

Configure authentication

Provisioning Services 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

    - security admin 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 security admin 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

Provisioning Services 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 use Active Directory for Provisioning Services administration roles.
  Note: Windows 2,000 Domains are not supported.
- Use Windows groups for security. Select this option if you are on a single server or in a Workgroup. This option enables you to use the Local User/Groups on that particular server for Provisioning Services administration roles.

Console users do not directly access the database.

Minimum permissions required for more Provisioning Services functionality include:

- Provisioning Services 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 Provisioning Services Console user account configured as a XenDesktop administrator and added to a PVS Site Admin group or higher
  - Active Directory Create Accounts permission to create accounts in the Console. To use existing accounts, Active Directory accounts have to exist in a known OU for selection
  - 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 Provisioning Services Console, Imaging wizard, PowerShell snap-in and MCLI use Kerberos authentication when communicating with the Provisioning Services 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 Provisioning Services SOAP service is running in. If the registration is not performed, the Kerberos authentication fails and Provisioning Services falls back to using NTLM authentication.

The Provisioning Services 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

Installing Provisioning Services Server software

December 28, 2018

This installation procedure is for new Provisioning Services implementations. For upgrade tasks, refer to the Upgrading from Previous Releases section. The software can also be installed silently (refer to the **Silent Install** section).

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

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

1. Click on the appropriate platform-specific install option. The **Provisioning Services 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 Provisioning Services 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 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 rerun to install more components later, or rerun on a different computer to install select components on a separate computer.
11. Click **Finish** to exit the Installation Wizard. The Provisioning Services Configuration Wizard automatically opens.

> **Tip**
>
> Although Provisioning Services does not require that you restart the server after installing the product software, in some instances, a Microsoft message may appear to request 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.

Silent product software installs

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

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

To set a different destination, use the following option:

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

Configuring the farm

January 24, 2019

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\Provisioning Services.

Starting the Configuration Wizard

The Configuration Wizard starts automatically after Provisioning Services software is installed. The wizard can also be started by selecting **Start > All Programs > Citrix > Provisioning Services \ > Provisioning Services Configuration Wizard**.

> **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.

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 needs to download a boot file from a TFTP server.

   Select the network service to provide target devices with PXE boot information:

   - If you choose to use this Provisioning Server 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)
     - Provisioning Services PXE Service
   - If Provisioning Services will 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, otherwise the farm name may display truncated 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 on to 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:

   - On the **Database Server** dialog, click **Browse** to open the **SQL Servers** dialog.
   - From the list of SQL Servers, select the name of the server where this database exists and the instance to use (to use the default instance, SQLEXPRESS, leave the instance name blank). In a test environment, this may be a staged database.

  Note: When rerunning the Configuration Wizard to add more 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'.
- Click **Next**. If this is a new farm, continue on to the "Defining a Farm"procedure.

2. To change the database to a new database:

   - On the old database server, perform a backup of the database to a file.
   - On the new database server, restore the database from the backup file.
   - Run the Configuration Wizard on each Provisioning Server.
   - Select **Join existing farm** on the **Farm Configuration** dialog.
   - Enter the new database server and instance on the **Database Server** dialog.
   - Select the restored database on the **Existing Farm** dialog.
   - Select the site that the Server was previously a member of on the **Site** dialog.
   - 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. Also, be aware that 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 to be a member, 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 to verify 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 displays and does not allow you to 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 selection network cards for the Stream Service.

Creating self-signed certificates for Linux streaming

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

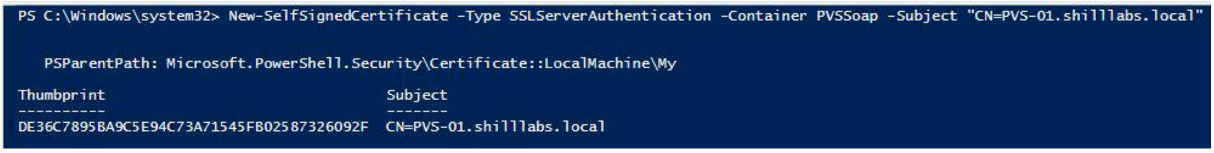
Using the PVS Configuration Wizard, you can choose to add the proper certificate from the PVSSoap container, specifically for Linux Desktops.

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 will be placed into the PVSSoap container:

```
#New-SelfSignedCertificate –Type SSLServerAuthentication –Container PVSSoap –Subject “CN=PVS-01.fqdn” –CertStoreLocation “Cert:\LocalMachine\My” –KeyExportPolicy Exportable
<!--NeedCopy-->
```

> **Important**
>
> This command requires PowerShell 5.0 or later. Windows Server 2012 comes with PowerShell 4.0 which does not accept the command described in this section.



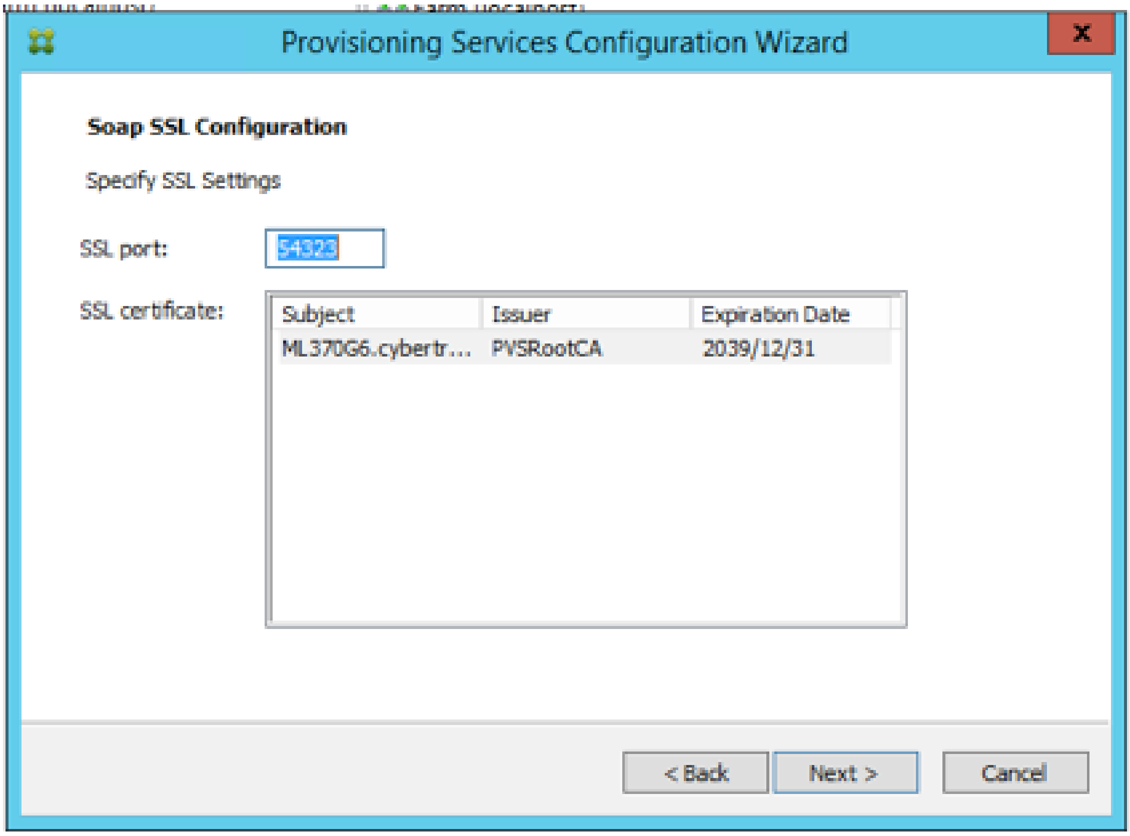
```
PS C:\Windows\system32> New-SelfSignedCertificate -Type SSLServerAuthentication -Container PVSSoap -Subject "CN=PVS-01.shilllabs.local"


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

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

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

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



Provisioning Services Configuration Wizard

Soap SSL Configuration

Specify SSL Settings

SSL port: 54323

SSL certificate:

Subject	Issuer	Expiration Date
ML370G6.cybertr…	PVSRootCA	2039/12/31

> **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:

2. 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 Provisioning Services was installed on this server, and the default location is:

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

you must 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.

1. Click **Next**.
2. Select **Provisioning Servers** to use for the boot process:
   - 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.
   - Optionally, highlight the IP address of the Provisioning Server that target devices boot from, then click **Advanced**. The Advanced Stream Servers Boot List appears.

The following table describes advanced settings that you can choose from. After making your selections, click **OK** to exit the dialog, then click **Next** to continue.

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. This enables debugging of target device drivers that exhibit timing or boot behavior problems.

Field	Description
Advanced Memory Support	This setting enables the bootstrap to work with newer Windows OS versions and is enabled by default. Only 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 the Restore Network Connections option is selected. 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 Provisioning Server that responds is used. In non-HA configurations, this time-out simply defines how often to retry the single available Provisioning Server with the initial login request. This time-out defines how quickly the round-robin routine switches from one Provisioning Server to the next in trying to find an active Provisioning Server. The valid range is from 1,000 milliseconds 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 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 Provisioning Server to the other Provisioning Servers to determine if they are indeed online or not. The valid range is from 1,000 milliseconds to 60,000 milliseconds.

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.

Preparing a master target device for imaging

May 13, 2021

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

> **Important**
>
> Citrix recommends that you install 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 is imaged to the vDisk. If necessary, after imaging, the hard disk can be removed from the master target device.

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 use BDM, the master target (prior to vDisk creation) should match the BDM configuration because end target devices use that configuration when booting.

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

If target devices are sharing 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 be prepared correctly and to install all software on it in the correct order.

Follow the instructions below after installing and configuring the Provisioning Server and creating target devices.

Software must be installed on the Master Target Device in the following order:

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

Applications can be installed before or after the target device software is installed. If target devices are members of a domain, and will share a vDisk, more configuration steps must be completed (refer to Managing Domain Computer Accounts, before proceeding with the installation).

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

Configuring a master target device's BIOS

The following steps describe how to configure the target devices 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, reboot the target device and enter the system's BIOS setup. (To get to BIOS setup, press the F1, F2, F10, or 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 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.

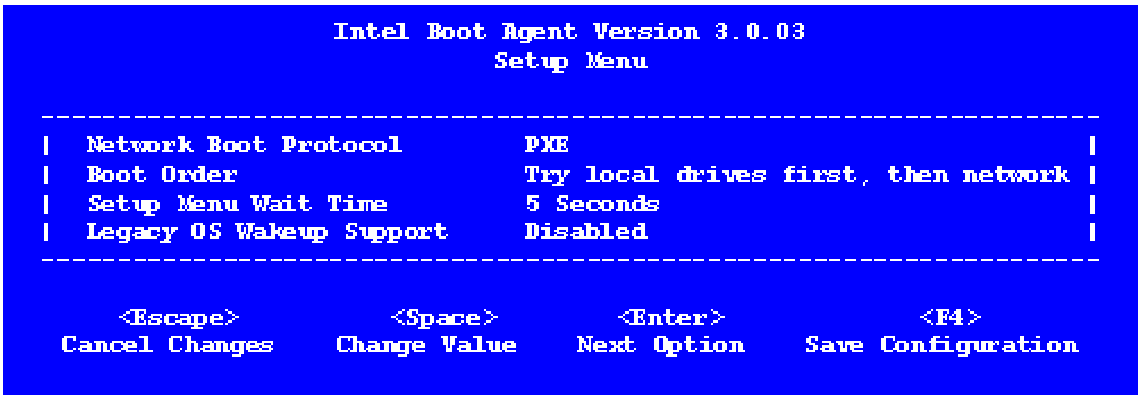
1. Reboot the Master Target Device.

2. Configure the network adapter's BIOS extension through setup.

   During the system boot, the network adapter's BIOS extension presents 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.) 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:



```
                    Intel Boot Agent Version 3.0.03
                              Setup Menu

 ----------------------------------------------------------------------
 |  Network Boot Protocol         PXE                                 |
 |  Boot Order                    Try local drives first, then network |
 |  Setup Menu Wait Time          5 Seconds                           |
 |  Legacy OS Wakeup Support      Disabled                            |
 ----------------------------------------------------------------------

      <Escape>           <Space>          <Enter>            <F4>
   Cancel Changes     Change Value     Next Option     Save Configuration
```

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 OEM NIC teaming software before installing target device software.

Provisioning Services target device software components comprise:

- **Provisioning Services Virtual Disk**: the virtual media used to store the disk components of the operating system and applications.
- **Provisioning Services Network Stack:** a proprietary filter driver that is loaded over the NIC driver, allowing communications between the target devices and the Provisioning Server.
- **Provisioning Services SCSI Miniport Virtual Adapter**: the driver that allows the vDisk to be mounted to the operating system on the target device.
- **Provisioning Services 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.

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

Note: When installing Provisioning Services 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 Provisioning Services 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 click
   Cancel to cancel the installation and roll-back any system modifications. Close any Windows Logo messages that appear.
10. The 'Installation Wizard Completed'message displays in the dialog when the components and options have successfully been installed. Close the wizard window. If both .NET 4.5 or newer is installed and Windows Automount is enabled, the Imaging Wizard starts 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.

Assigning vDisks to target devices

December 28, 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. Select the appropriate vDisk to boot.

If one or more versions exist for a vDisk, 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'in the Administrator's Guide. For Maintenance and Test devices, the State of any non-production versions are labeled.

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 that contains one or more target devices that use personal vDisks. The dialog provides the option to continue by acknowledging that the vDisk is assigned those devices that are not currently assigned a personal vDisk. Also, target devices that use personal vDisks cannot inherit the properties of a target device that doesn't 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, expand **Stores** to display the vDisk to be assigned 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 vDisks to assign to this target device, select a specific store or server under the Filter options. Or, 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.

Configuring the bootstrap file from the console

December 20, 2019

For the Provisioning Server to start a target device, a boot file is downloaded by the Provisioning Services MBA or PXE-compliant boot ROM. This file must be configured so that it contains the information needed to communicate with the servers.

Use the **Configure Bootstrap** dialog, located in the server's contextual menu, 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 fields:

General tab: Configure bootstrap

Field	Description
Bootstrap File	The currently selected boot file displays. If you want to select a different boot file to configure, click the **Add** button or Read Servers from Database button.
IP Settings	The IP Address, Subnet Mask, Gateway, and Port for up to four Provisioning Servers.
Add	Click the **Add** button to include a Provisioning Server to the file. Up to four Provisioning Servers are specified.
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 process clears the list then populates the list with the first four servers found in the database.

Target device IP: Configure bootstrap

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 a primary and secondary DNS and Domain.

Server lookup: Configure bootstrap

Field	Description
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 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 is the server that the target device attempts to boot from.

Options tab: Configure bootstrap

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.
Network recovery method	**Restore Network Connections** —Selecting this option results in the target device attempting indefinitely to restore its connection to the Provisioning Server. **Reboot to Hard Drive** —A hard drive must exist on the target device. Selecting this option instructs the target device to perform a hardware reset to force a reboot after failing to re-establish communications. The user determines the number of seconds to wait before rebooting. Assuming the network connection cannot be established, PXE fails, and the system reboots to the local hard drive. The default number of seconds is 50, to be compatible with HA configurations.

Field	Description
Login 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 Provisioning 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 switches from one Provisioning Server to the next in trying to find an active Provisioning Server. The valid range is from 1,000 milliseconds to 60,000 milliseconds.
Login general timeout	Enter the time-out, in milliseconds, for all login associated packets, except the initial login polling time-out. This time-out is longer than the polling time-out, because the Provisioning Server needs time to contact all associated servers. Some servers may be down and require retries and time-outs from the Provisioning Server to the other Provisioning Servers to determine if they are indeed online or not. The valid range is from 1,000 milliseconds to 60,000 milliseconds.

Configuring the bootstrap File

1. In the Console, select a Provisioning Server within the **Servers** folder in the tree, then select **Configure bootstrap** from the **Actions** pane or the context menu. The **Configure Bootstrap** dialog appears.

   Select the boot file that was copied to the directory you selected during the Provisioning Server setup. Because the server returns the list of bootstrap files found under **Provisioning Services ProgramData**, the server must be active for the **Configure Bootstrap** menu item to appear.

   Important:

   If a previous version of Provisioning services was installed on this server, you must change the default location from:

C:\Program Files\Citrix\Provisioning Services

to:

C:\Documents and Settings\All Users\Application Data\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; 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. Provisioning Services 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 its 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 cannot be established, PXE fails and the system reboots to the local hard drive. The default number of seconds is 50. Click the **Browse** button to search for and select the folder created in Step 1, or enter a full path or UNC name.

   Note: If the partition containing the vDisks is formatted as a FAT file system, a message displays a warning that this could result in suboptimal performance. Citrix recommends using NTFS to format the partition containing the vDisks. Do not change the address in the **Port** field.

   Caution: 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 switches from one server to the next, in trying to find an active server. The valid range is from 1,000 milliseconds to 60,000 milliseconds.

   Login General Timeout

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

6. Click **OK** to save your changes.

Configure PVS-Accelerator

April 15, 2021

PVS-Accelerator enables a PVS proxy to reside in Dom0 (XenServer's Control Domain) on a XenServer host where streaming of a PVS 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 PVS-Accelerator:

- PVS and XenServer provide an improved functional paradigm by providing a unique value available when used together.
- PVS 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 PVS 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(s). There are no additional dependencies on the installer.

Citrix recommends that you do not disable the PVS-Accelerator feature on a VM using the XenServer console. When disabled using this method, PVS fails to recognize the configuration change and continues to believe that the PVS-Accelerator feature is enabled on that VM. If you want to disable this feature for a single device, see the sections Enabling or disabling PVS Accelerator for individual devices and Disabling PVS-Accelerator for all devices on a host.

Using PVS-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. To use this feature, an optional package must be installed on the XenServer host(s). There are no additional dependencies on the installer.

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

Consider the following when using this feature with XenServer:

- A XenServer PVS Site object must be created and configured with the storage repository (SR) before the PVS Console can establish a proxy connection on the VM.
- PVS calls the XenServer API to check if the proxy feature is enabled before it exposes any PVS/XenServer proxy interfaces.
- PVS configures the XenServer proxy for devices using the XenDesktop Setup Wizard and the Streamed VM Setup Wizard.
- PVS targets are aware of the their proxy status; once the feature is installed, no additional configuration tasks are required.
- After re-installing XenServer, the PVS-Accelerator cache remains configured in the PVS database. This causes an error in the VM setup wizard because PVS assumes that the cache still exists. To resolve this issue, delete and then add the XenServer host using the PVS console. This enables PVS to clear the stored cache configuration. After the stored cache configuration has been cleared, the administrator can create a new one in XenCenter.

> **Tip**
>
> In environments where two PVS 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 PVS-Accelerator

Use the XenDesktop Setup Wizard and the Streaming Wizard to access the PVS-Accelerator 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.

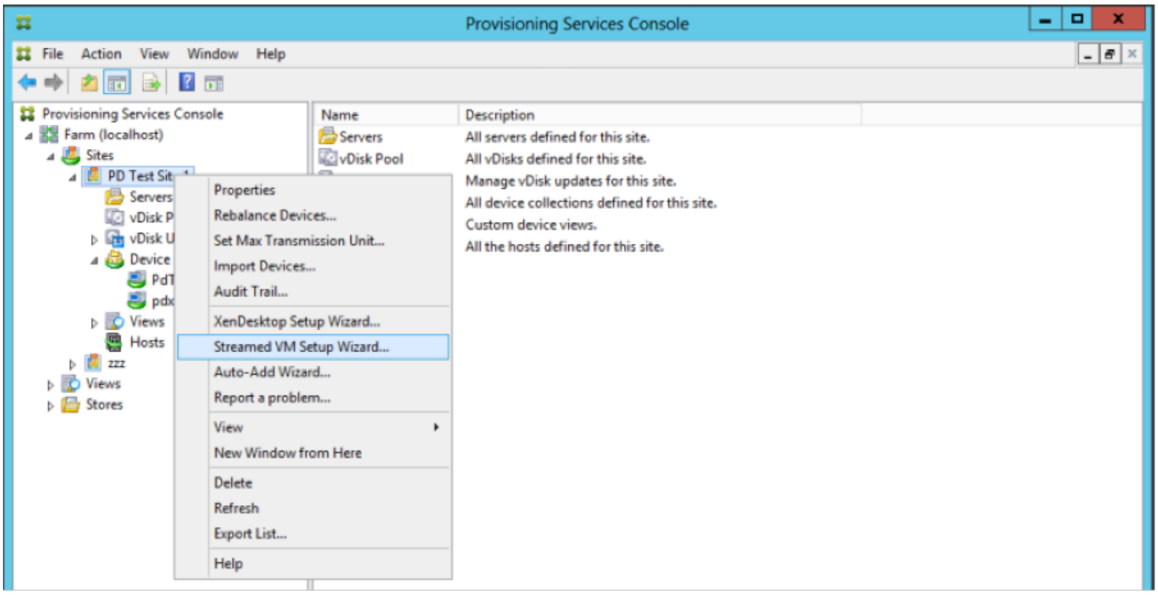
> **Note**
>
> This feature is only supported on XenServer that has the capability installed. UI changes captured in this section only apply when you are using that type of hypervisor.

When a proxy cache configuration (i.e., PVS-Accelerator is enabled) is tied to a PVS server, and you reinstall XenServer on the host that had this feature enabled, PVS and XenServer become out of sync. This occurs because the reinstallation of XenServer wipes the previously configured proxy cache configuration.

> In this scenario, PVS assumes that the proxy cache configuration still exists, and when the Streamed VM Setup Wizard is used, it fails, indicating 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. After accomplishing this, reconfigure PVS and setup the cache again.

To configure PVS-Accelerator, select one of the Wizards based on how you intend to use it (**XenDesktop Setup Wizard** or **Streamed VM Setup Wizard**) in the PVS Console:

1. Navigate to a site.
2. Select the site, then right click to expose a contextual menu. Select the appropriate Wizard based on how you intend to use the PVS-Accelerator feature:



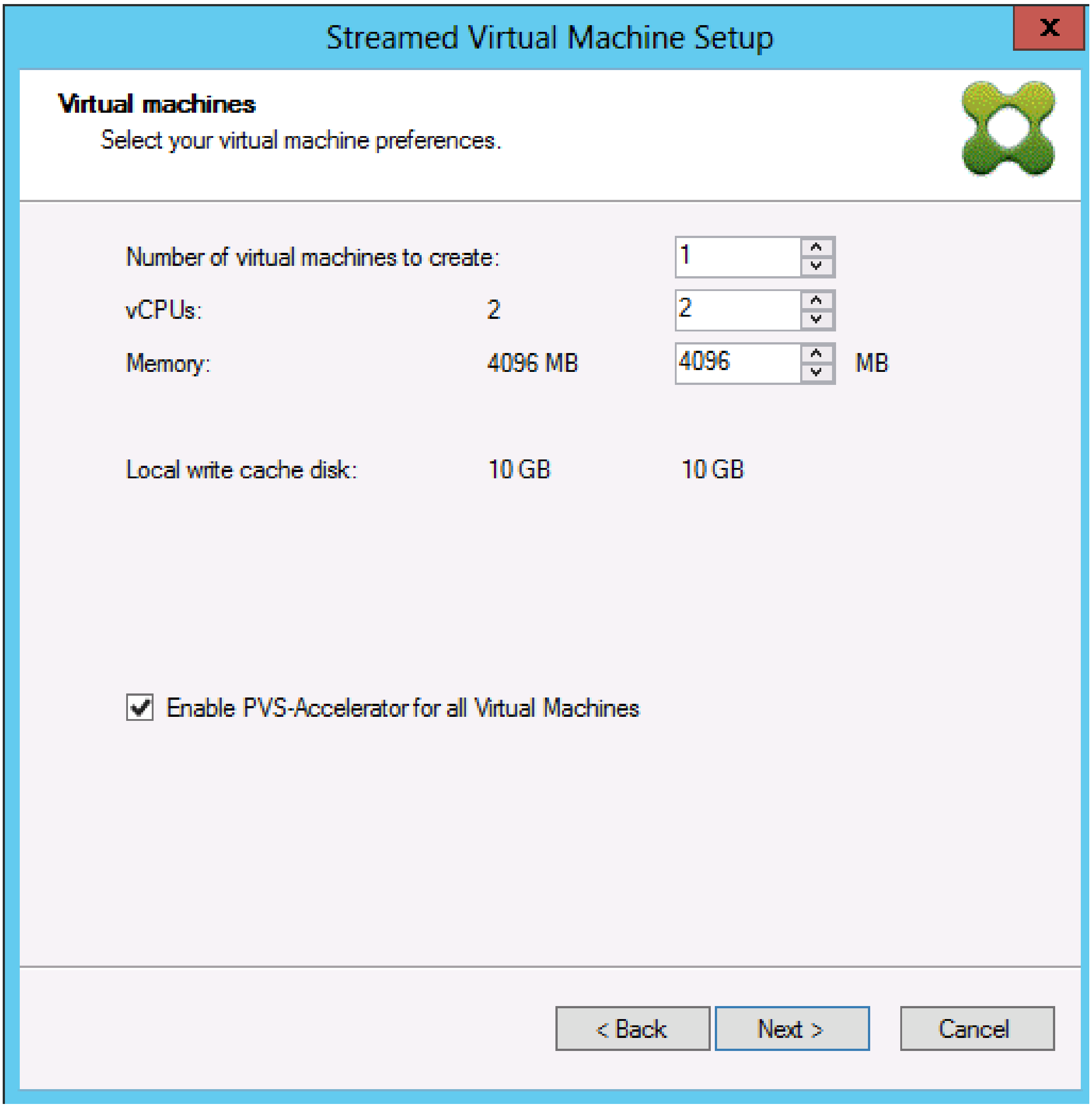
Name	Description
Servers	All servers defined for this site.
vDisk Pool	All vDisks defined for this site.
	Manage vDisk updates for this site.
	All device collections defined for this site.
	Custom device views.
	All the hosts defined for this site.

Using Wizards to configure PVS-Accelerator

To use PVS-Accelerator, first determine how you will use it. If you are:

- configuring VMs running on a hypervisor controlled by XenDesktop, use the **XenDesktop 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**:


Streamed Virtual Machine Setup

Virtual machines

Select your virtual machine preferences.

Number of virtual machines to create: 1

vCPUs: 2 2

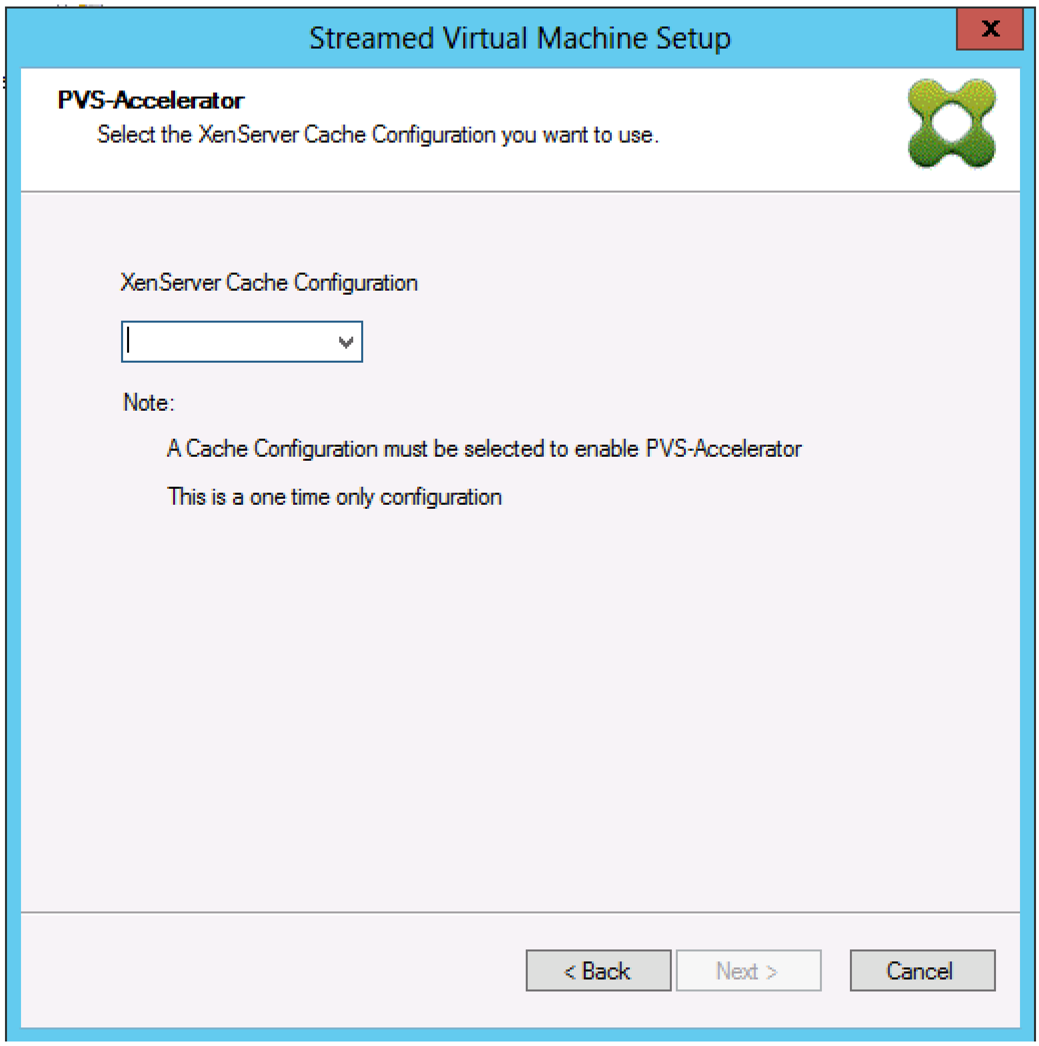
Memory: 4096 MB 4096 MB

Local write cache disk: 10 GB 10 GB

☑ 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**:



PVS-Accelerator

Select the XenServer Cache Configuration you want to use.

XenServer Cache Configuration

Note:

A Cache Configuration must be selected to enable PVS-Accelerator

This is a one time only configuration

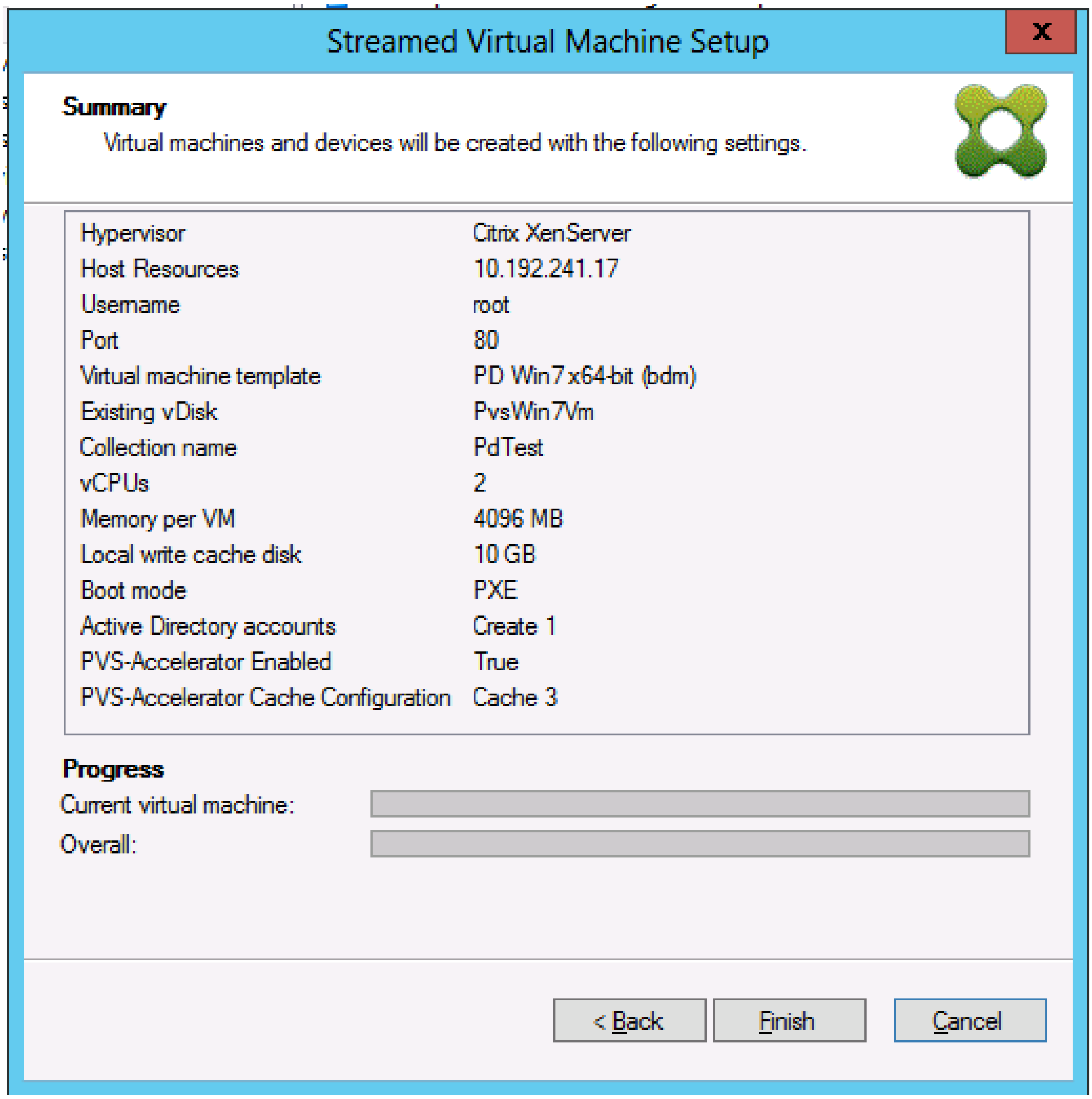
> **Tip**
>
> The Wizard allows you to select the XenServer PVS Site to which you want to apply PVS-Accelerator functionality. In the XenServer screen, a drop down list displays the list of all the PVS Site objects on XenServer that have been configured but not yet associated with a PVS site.

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

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

After using one of the Wizards to configure the PVS-Accelerator feature, the Summary screen appears illustrating the current state; use this screen to determine if it is enabled, and the current cache configuration associated with it.

Click **Finish** to apply the configuration:



Summary

Virtual machines and devices will be created with the following settings.

Hypervisor	Citrix XenServer
Host Resources	10.192.241.17
Username	root
Port	80
Virtual machine template	PD Win7 x64-bit (bdm)
Existing vDisk	PvsWin7Vm
Collection name	PdTest
vCPUs	2
Memory per VM	4096 MB
Local write cache disk	10 GB
Boot mode	PXE
Active Directory accounts	Create 1
PVS-Accelerator Enabled	True
PVS-Accelerator Cache Configuration	Cache 3

Progress

Current virtual machine:

Overall:

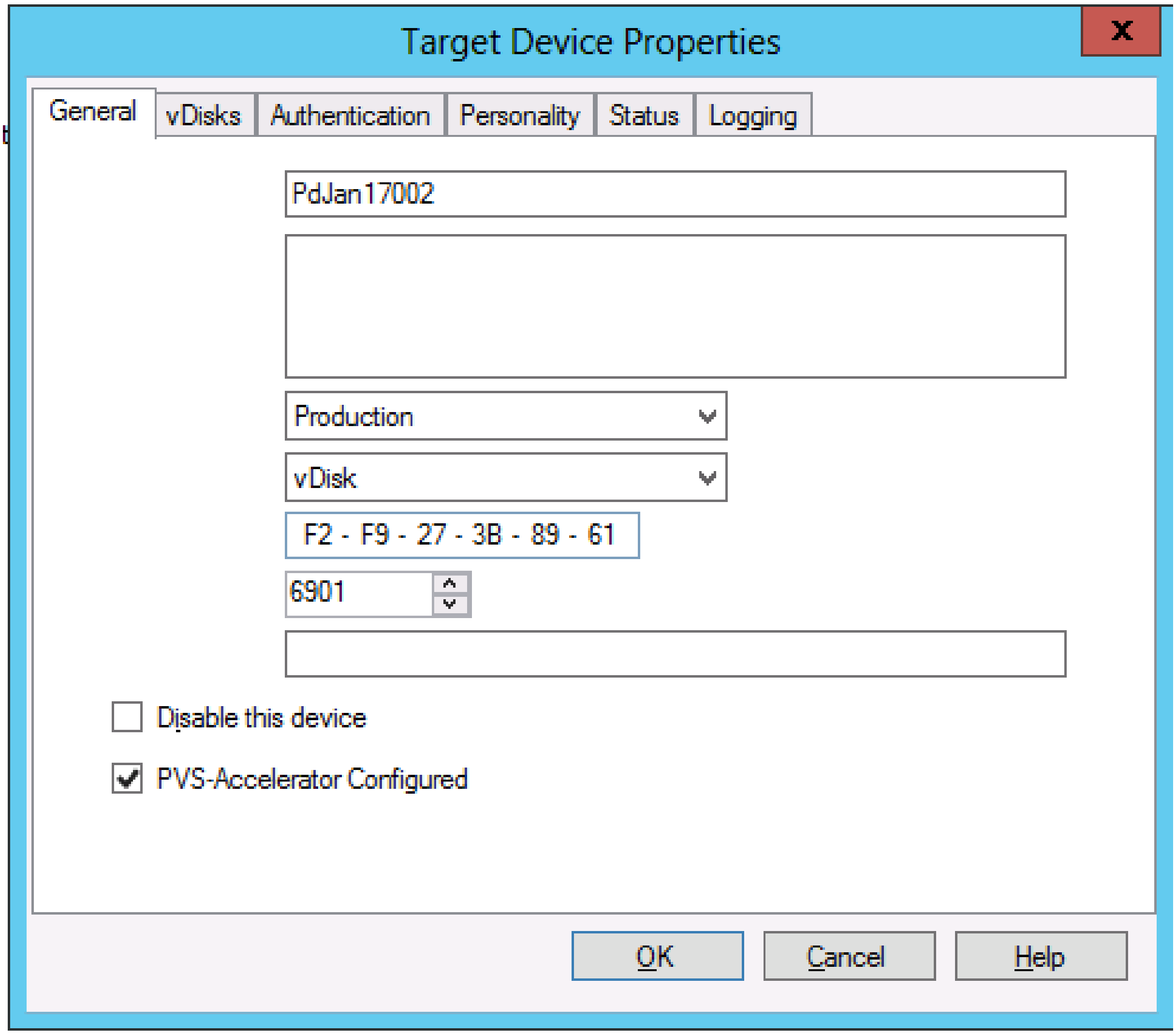
Enabling or disabling PVS-Accelerator for individual devices

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

To enable or disable PVS-Accelerator 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.



PdJan17002

Production

vDisk

F2 - F9 - 27 - 3B - 89 - 61

6901

□ Disable this device

☑ PVS-Accelerator Configured

Disabling PVS-Accelerator for all devices on a host

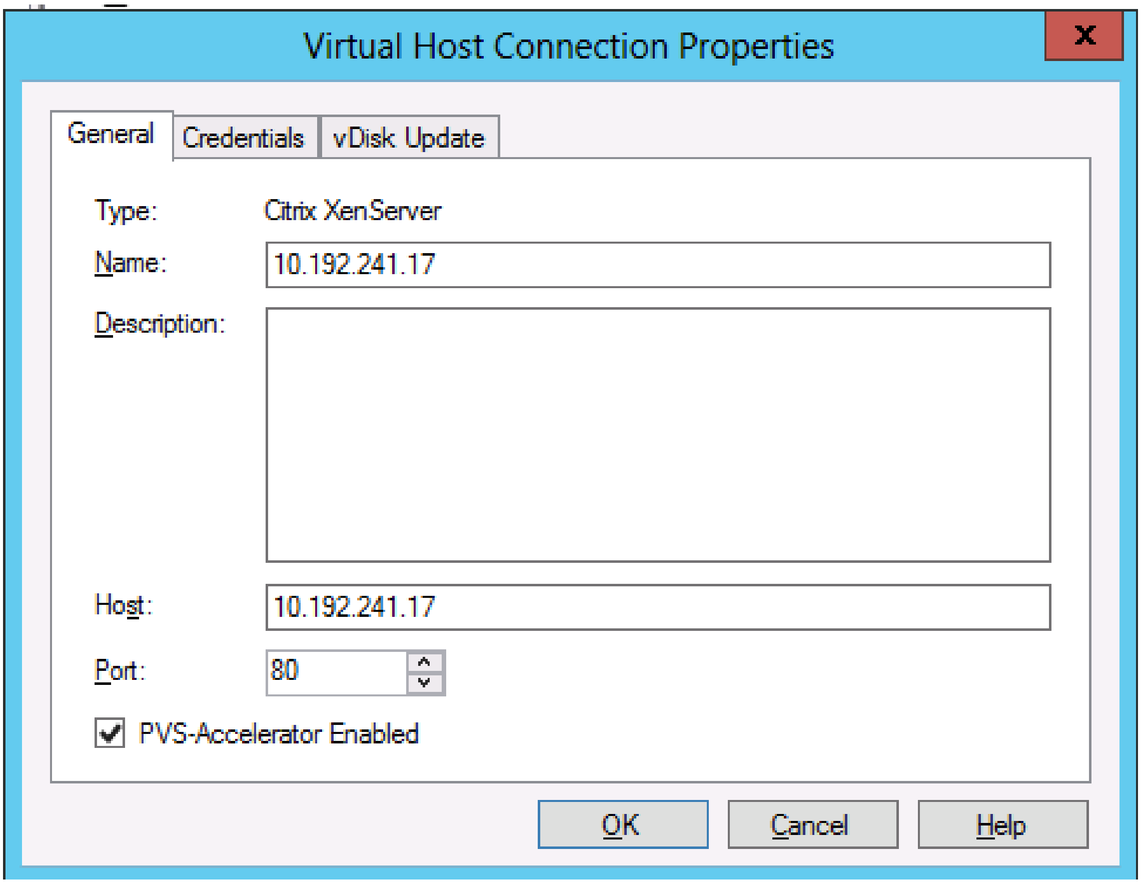
If PVS-Accelerator was enabled for a host, you can disable it using the **Virtual Host Connection Properties** screen for all devices on the specified host.

> **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 (XenDesktop Setup Wizard or Streamed Wizard) while creating new devices.

To disable PVS-Accelerator 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**.



Type: Citrix XenServer

Name: 10.192.241.17

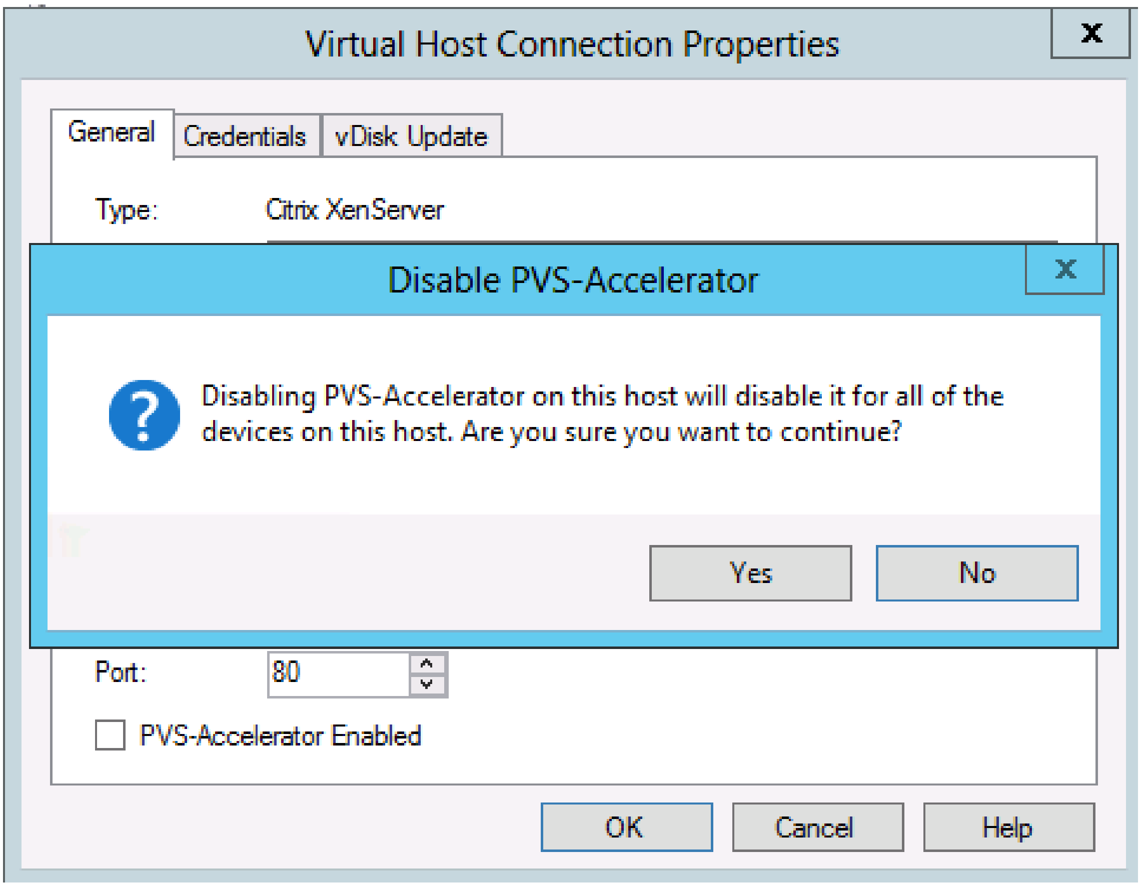
Description:

Host: 10.192.241.17

Port: 80

☑ PVS-Accelerator Enabled

3. You will be prompted to confirm the following action:


Virtual Host Connection Properties

Type: Citrix XenServer

Disable PVS-Accelerator

Disabling PVS-Accelerator on this host will disable it for all of the devices on this host. Are you sure you want to continue?

Port: 80

□ PVS-Accelerator Enabled

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

Using the Provisioning Services Console

December 28, 2018

Use the Provisioning Services Console to manage components within a Provisioning Services farm. The Console can be installed on any machine that can access the farm.

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).

From the Start menu, select:

`All Programs\>Citrix\>Provisioning Services\ > Citrix Provisioning Console`

The Console's main window appears.

> **Tip**
>
> To connect to a farm refer to Farm Tasks.

Understanding the Console window

On the main Console window, you can perform tasks for setting up, modifying, tracking, deleting, and defining the relationships among vDisks. These relationships extend to 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.

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 are dependent on the role that you are assigned.

Common Action Menu Options

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. 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.
5. Click **Save** to save the file.

Help

Select an object in the Console, then select **Help** from the **Action** menu to display information about that object.

View Options

To customize a Console view:

1. Select **View**, then select either Add/Remove Columns…or Customize….
2. If you selected:
    - Add/Remove Columns…, use the **Add and Remove** buttons to select which columns to display.
    - Customize…, select the check box next to each MMC and Snap-in view option that should display in the Console window.
3. Click **OK**. The Console view refreshes to display the view options selected.

Performing tasks in the Console

December 28, 2018

Action menu

Select object-related tasks from the **Action** menu, including boot, restart, send message, view properties, copy, or paste properties.

Right-click (context) Menu

Right-click a managed object to select object-related tasks. For a complete list of tasks, refer to that object's management chapter within this guide.

Using 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. (Any vDisks assignments that were specific to this server and any store information will be lost.).

Using 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 in the tree or details pane that you want to paste properties to, then select **Paste**.

Using 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 **Add**. 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.

Farm properties

December 28, 2018

The following tables identify and describe properties on each tab of the **Farm Properties** dialog.

General tab

Name	Enter or edit the name of this farm.
Description	Enter or edit a description for this farm.

Security tab

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

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, in this release, if you type MY_DOMAIN\Builtin*, you get all groups, including 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.
Remove button	Click the **Remove** button to remove existing groups from this farm. Highlight the groups to which privileges should not apply.

Licensing tab

Note: Changing licensing properties requires that you restart the Provisioning Services Stream Service on each Provisioning Server for licensing changes to take effect.

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

Auto-Add	Use this checkbox for the Auto-add feature. Select the site for new target devices from the Add new devices to this site drop-down menu. If the No default site is chosen for the default site setting, then the site of that Provisioning Server that logs in the target device is used during auto-added. 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 when the connection to the database is lost.

vDisk Version tab

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 will automatically be set to Maintenance or Test. If a Maintenance version exists, an automatic merge will not be 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

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

Farm tasks

December 28, 2018

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 more 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. To open the dialog, right-click on the **Provisioning Services Console** icon in the tree, then select the **Manage Connections…** menu option.

Managing sites

December 28, 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 site

1. Right-click on the sites folder in the farm where you want to add the new site. The **Site Properties** dialog appears.
2. On the **General** tab, type the name and a description for the site in the appropriate text boxes.
3. On the **Security** tab, click **Add** to add security groups that have the site administrator rights in this site. The **Add Security Group** dialog appears.
4. 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

Field/Button	Description
Name	Type the name of this site in the textbox.
Description	Optional. Type the description of this site in the textbox.

Security Tab

Field/Button	Description
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 checkbox**.

Field/Button	Description
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 checkbox**.

MAK tab

Field/Button	Description
Enter the administrator credentials used for Multiple Activation Key enabled Devices	MAK administrator credentials must be entered before target devices using MAK can be activated. The user must have administrator rights on all target devices that use MAK enabled vDisks and on all Provisioning Servers that stream those target devices.

After entering the following the user name and password, click **OK**.

> **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 reappears.

Options tab

Field/Button	Description
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.

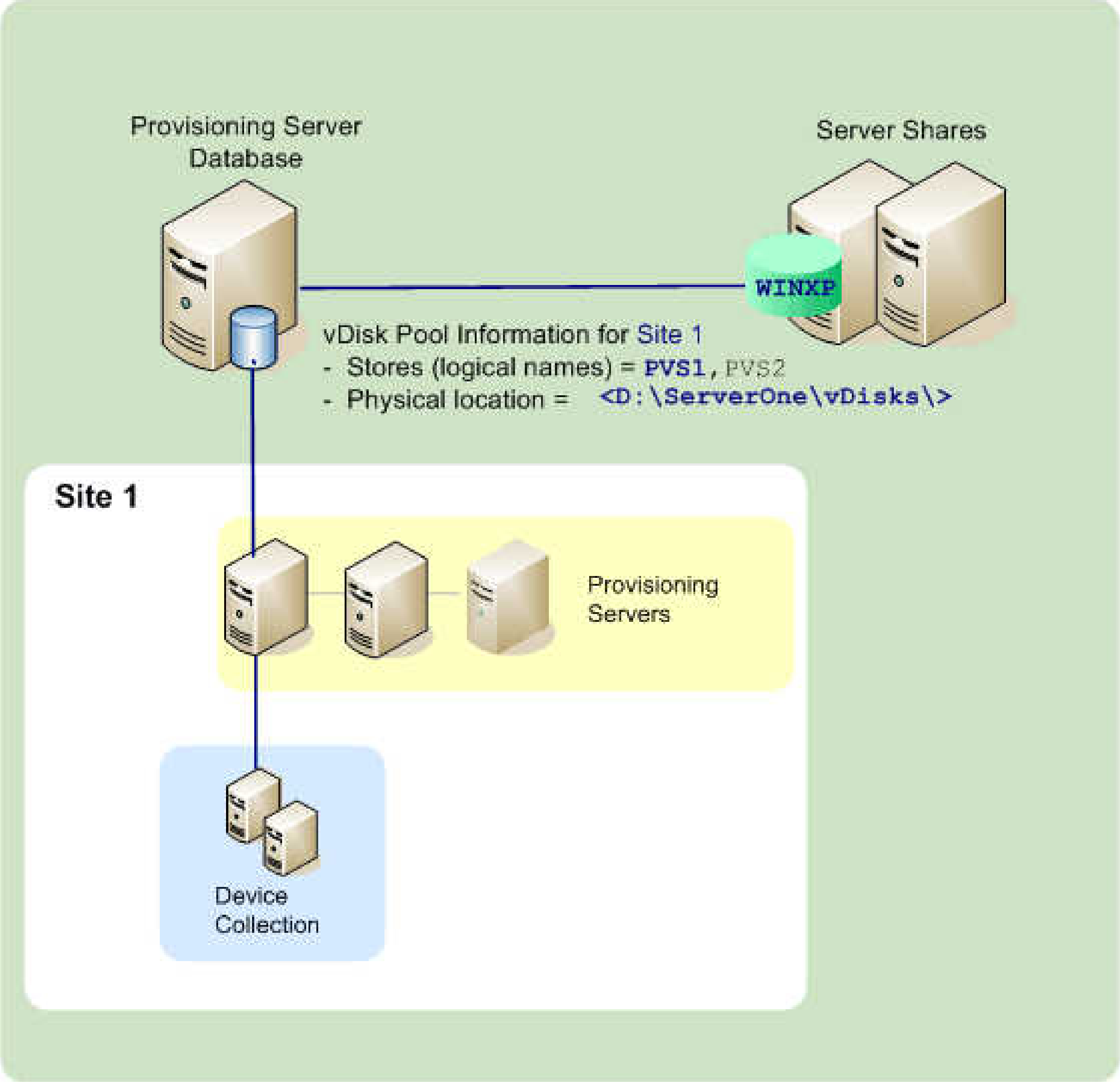
vDisk update tab

Field/Button	Description
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.

Managing stores

January 3, 2019

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 to serve vDisks to target devices.


Provisioning Server Database
Server Shares
WINXP
vDisk Pool Information for Site 1
- Stores (logical names) = PVS1, PVS2
- Physical location = <D:\ServerOne\vDisks\>
Site 1
Provisioning Servers
Device Collection

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

Separating the physical paths to a vDisks storage location allows for greater flexibility within a farm configuration, particularly if the farm is configured to be highly available. In a highly available implementation, if the active Provisioning Server in a site fails, the target device can get its 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 when the 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 because the default path is not valid for that server an override path can be set in the store properties for that particular server. Provisioning Servers use either the default path 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 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 acts 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 the browse button, and then clicking **Create New Folder**. If the user is a site administrator, only those sites that they administer appear in the list.
7. The write cache path for the selected store display under the paths list. Optionally, a new store cache folder can be created by clicking the browse button, and then clicking **Create New Folder**. More write cache paths can be added for use by the store by clicking **Add**. Entering more than one write cache paths allows for 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, 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. Use the **Store Properties** dialog to:

- Name and provide a description of the store
- Select the owner of the store (the site which manages the store)
- Provide a default path to the store (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

Field	Description
Name	View, type the logical name for this store. For example, PVS-1.
Description	View or type a description of this store.

Field	Description
Site that acts as owner of this store	Optional. View or scroll to select the site that acts as owner of this store. This feature allows a farm administrator to give one site's administrators, special permission to manage the store. These rights are normally reserved for farm administrators.

Paths

Field	Description
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 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

Field	Description
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.
Validate	Click to validate store path selections from the **Validate Store Paths** dialog. The validation results display under the **Status** column.

Provisioning Server properties

December 28, 2018

On the Console, the **Provisioning Server Properties** dialog allows you to modify Provisioning Server configuration settings. To view an existing Provisioning Server's 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

Note: Provisioning Services displays a message if a change made on a Provisioning Server Properties dialog requires that the server be rebooted.

General

- Name and Description

Displays the name of the Provisioning Server and a brief description. The maximum length for the server name is 15 characters. Do not enter FQDN for the server name.

- Power Rating

A power rating is assigned to each server, which is then used when determining which server is least busy. The scale to use is defined by the administrator.

For example, an administrator may decide to rate all servers on a scale of 1–10, or on a scale of 100–1000. Using the scale of 1–10, a server with a rating of 2 is considered twice as powerful as a server with a rating of 1; therefore it would be assigned twice as many target devices. Likewise, when using a scale of 100–1000, a server with a power rating of 200 is considered twice as powerful as a server with the rating of 100; therefore it would also be assigned twice as many target devices.

Using the default setting of 1.0 for all servers results in even device loading across servers. In this case, the load balancing algorithm does not account for individual server power.

Ratings can range between 0.1-1000.0. 1.0 is the default.

Note: The load balancing method is defined in vDisk Load Balancing dialog.

- Log events to the server's Window Event Log

Select this option if you want this Provisioning Server's events to be logged in the Windows Event log.

- Advanced Server Properties

Server tab

Threads per port —Number of threads in the thread pool that service UDP packets received on a given UDP port. Between four and eight are reasonable settings. Larger numbers of threads allow more target device requests to be processed simultaneously, but consumes more system resources.

Buffers per thread —Number of packet buffers allocated for every thread in a thread pool. 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 Provisioning Services 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 attempts to write its status information every (Server cache timeout/2) second, that is, at twice the timeout rate. A shorter server cache timeout value allows servers to detect offline servers more quickly, at the cost of extra database processing. A longer Server cache timeout period reduces database load at the cost of a longer period to detect lost servers.

Local and Remote 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 PVS 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 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 PVS Service, better performance can be achieved with these types of devices.

Local device is defined as any device starting with a drive letter. Remote is defined as any device starting with a UNC server name. This is 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 1–3 for the remote limit may be necessary to achieve the best performance with the share. If you are going to 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 the PVS Service to run without limits. This might be desirable on fast local drives.

If a network share is overloaded, you 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.

Network tab

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. Provisioning Services currently does not 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 (Provisioning Services 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, that is, only 32 packets can be in a single IO burst before an ACK is needed.

Socket communications —Enable non-blocking I/O for network communications.

Pacing tab

Boot pause seconds —The amount of time that the device will be told to pause if the Maximum devices booting limit has been reached. The device displays a message to the user and then wait Boot pause seconds before attempting to continue to boot. The device continues to check with the server every Boot pause seconds until the server allows the device to boot.

Maximum boot time —The amount of time a device will be considered in the booting state. Once a device starts to boot, the device is considered booting until the Maximum boot time has elapsed for that device. After this period, it will no longer be 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 allows 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

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

- 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.

Add —Add an IP address for the selected Provisioning Server.

Edit —Opens the **IP address** dialog so that 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

- Stores

Lists all stores (logical names representing physical paths to vDisks that are available to this Provisioning Server.

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.

- Store Properties (opens when **Add** or **Edit** is selected under **Stores**)

Store —The name of the store. This displays populated 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 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

- 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 be updated automatically, then set the time of day to check for updates.

Logging

- 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.

- 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.

Overview of Provisioning Server tasks

December 28, 2018

You typically perform the following tasks when managing 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.

- Copying and Pasting Server Properties
- Deleting a Server
- Starting, Stopping, or Restarting Provisioning Services on a Server
- Showing Server Connections
- Balancing Target Devices on a Server
- Checking for vDisk Access Updates
- Configuring Provisioning Servers Manually
- Auditing
- Configure Bootstrap

Deleting a Provisioning Server

January 23, 2020

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 Provisioning Server.

Note: If there are vDisks associated with the Provisioning Server being deleted, it is recommended that backup copies are created and stored 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 (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.

To decommission a Provisioning Server:

1. Verify if any provisioned clients are owned by the provisioning server you want to remove. If a provisioned client exists, shut it down.
2. If provisioned clients are owned by multiple servers, stop the stream service.
3. In the Citrix Provisioning console on the remaining provisioned server, the server appears as down, or, offline. Select the server, right click, and select **Delete** in the contextual menu.
4. Shutdown the system or uninstall the provisioning server.

Starting, stopping, or restarting Provisioning Services

May 12, 2022

> **Tip**
>
> Starting, stopping, or restarting Provisioning Services may result in unexpected behavior. Refer to Important considerations for more information.

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

1. Highlight the Provisioning Server in the Console, then select the Stream Services menu option from the Actions menu, right-click menu, or Actions pane. The Provisioning Server Control dialog appears.
2. Select from the following menu options:

Option	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

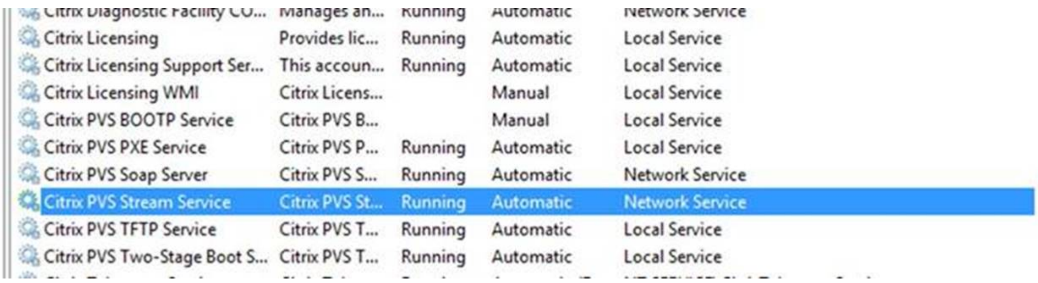
3. Highlight the Provisioning Servers that you want to take action on, then click that action's button.
4. Click Close to exit the dialog.

PVS console fails to restart or stop

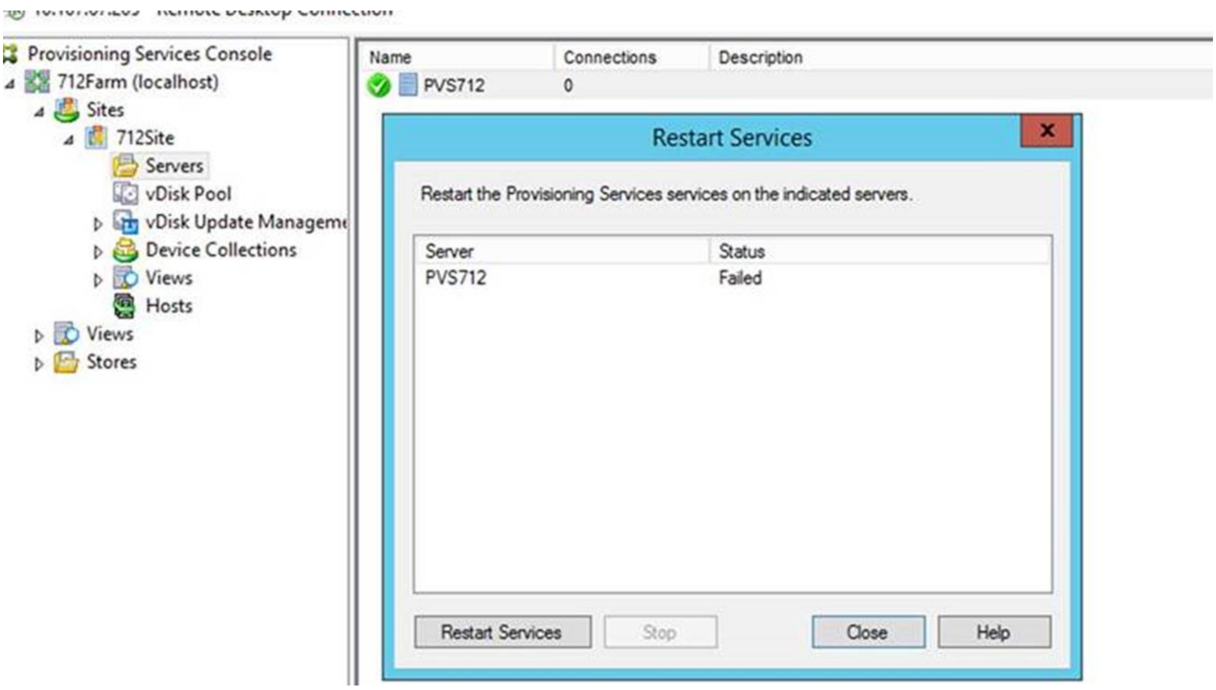
Sometimes, the PVS console may fail to restart or stop services when running a stream service with a network service account. When this occurs, the service may appear in the started state, however, the console prevents you from restarting or stopping the stream service.

> **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:



Citrix Diagnostic Facility CO...	Manages an...	Running	Automatic	Network Service
Citrix Licensing	Provides lic...	Running	Automatic	Local Service
Citrix Licensing Support Ser...	This accoun...	Running	Automatic	Local Service
Citrix Licensing WMI	Citrix Licens...		Manual	Local Service
Citrix PVS BOOTP Service	Citrix PVS B...		Manual	Local Service
Citrix PVS PXE Service	Citrix PVS P...	Running	Automatic	Local Service
Citrix PVS Soap Server	Citrix PVS S...	Running	Automatic	Network Service
Citrix PVS Stream Service	Citrix PVS St...	Running	Automatic	Network Service
Citrix PVS TFTP Service	Citrix PVS T...	Running	Automatic	Local Service
Citrix PVS Two-Stage Boot S...	Citrix PVS T...	Running	Automatic	Local Service



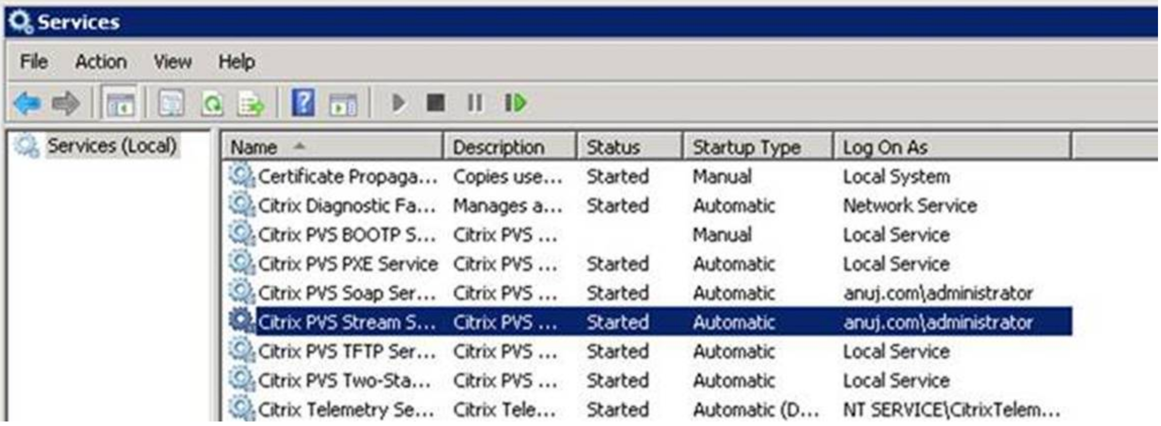
Name	Connections	Description
PVS712	0	

Restart Services

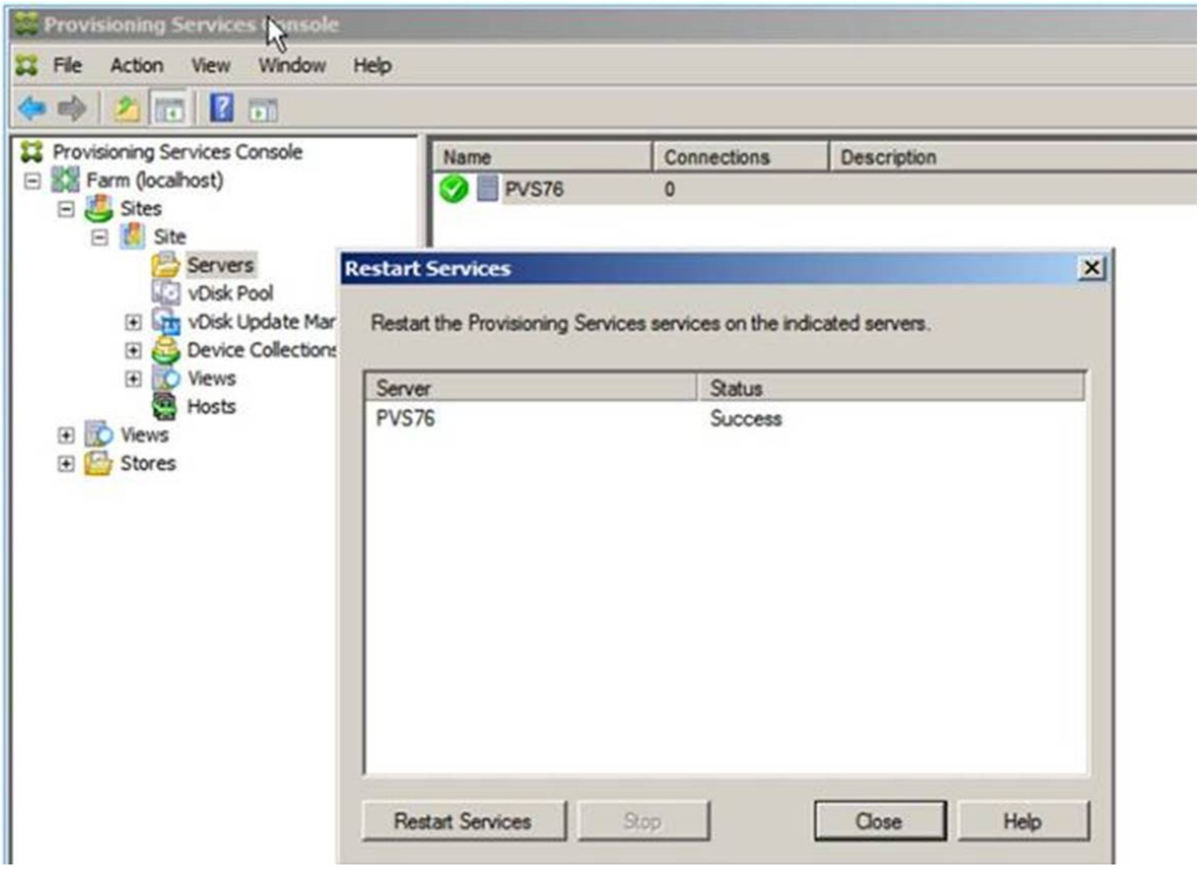
Restart the Provisioning Services services on the indicated servers.

Server	Status
PVS712	Failed

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 specific account (for example, anuj.com\administrator), the status appears as started, and you can restart or stop the services from the PVS console:



Name	Description	Status	Startup Type	Log On As
Certificate Propaga...	Copies use...	Started	Manual	Local System
Citrix Diagnostic Fa...	Manages a...	Started	Automatic	Network Service
Citrix PVS BOOTP S...	Citrix PVS ...		Manual	Local Service
Citrix PVS PXE Service	Citrix PVS ...	Started	Automatic	Local Service
Citrix PVS Soap Ser...	Citrix PVS ...	Started	Automatic	anuj.com\administrator
Citrix PVS Stream S...	Citrix PVS ...	Started	Automatic	anuj.com\administrator
Citrix PVS TFTP Ser...	Citrix PVS ...	Started	Automatic	Local Service
Citrix PVS Two-Sta...	Citrix PVS ...	Started	Automatic	Local Service
Citrix Telemetry Se...	Citrix Tele...	Started	Automatic (D...	NT SERVICE\CitrixTelem...



Restart the Provisioning Services services on the indicated servers.

Server	Status
PVS76	Success

Balancing the target device load on Provisioning Servers

December 28, 2018

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 appears.
2. After you enable load balancing for the vDisk, the following more 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 the least busy server. This setting is the default.
     - 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 if the trigger percent is exceeded. When enabled, Provisioning Services checks the trigger percent on each server approximately every 10 minutes. For example: If the trigger percent on this vDisk is set to 25%, rebalancing occurs within 10 minutes if this server has 25% more load in comparison to other servers that can provide this vDisk.

Note: The load balance algorithm determines the
Server Power setting of each server when determining load.

Load balancing fails if:

- less than five target devices are using a particular server
- the average number of target devices using all qualifying servers is less than five
- the number of target devices that are booting on a given server is more than 20% of the total number of devices connected to the server (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 more qualified servers are brought online, rebalancing occurs 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.

Note: Target devices that are not using a vDisk that is in HA mode cannot 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.

Disabling write cache to improve performance when using storage device drives

February 22, 2022

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 check box.
8. Click OK, then click OK again.
9. Close the Computer Management window, then the Administrative Tools window.
10. Right-click the Provisioning Server node in the Console, then click Restart service. Alternatively, you can also rerun the Configuration Wizard to restart the services, or manually restart the services through the **Windows Control Panel > Administrative Tools > Services** window. (At the Services window, right-click on the Stream Service, then select Start from the shortcut menu.)

Managing target devices

December 28, 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 boots 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

> **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.

Adding target devices to the database

December 28, 2018

To create 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 Devices 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.

Setting the target device as the template for this collection

March 2, 2022

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 are taken from the default template target device. No user interaction is required.

Creating a VM with nested virtualization

Sometimes, you might 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 set up 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.

> **Note:**
>
> Citrix Provisioning only supports Device Guard using Hyper-V 2016 and newer.

To configure a VM to use Device Guard:

1. Create the VM using the XenDesktop Setup Wizard.
2. After creating the VM, run the following command for each VM on the physical Hyper-V host to enable nested virtualization:

```
Set-VMProcessor -VMName <Target VM's Name> -
   ExposeVirtualizationExtensions $true
```

> **Tip**
>
> Refer to the Microsoft site for more information about nested virtualization.

Restarting target devices

February 17, 2022

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**.

Managing target device Personality

August 15, 2019

Normally, all target device's sharing the same virtual disk must have identical configurations. The Target Device Personality feature allows you to define data for specific target devices and make it available to the target device at boot time. This data can then be used by your custom applications and scripts for various 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 virtual disk. 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 is 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 64 Kb 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 devices using the Console
- Using Target Device Personality Data

Define personality data from a single target device using the Console

To define personality data for a single target device:

1. In the Console, right-click on the target device that you want to define personality data for, then select the Properties menu option.
2. Select the Personality tab.
3. Click the Add button. The Add/Edit Personality String dialog appears.
   Note: There is no fixed limit to the number of field names and associated strings you can add. However, the 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 64 Kb 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 devices using the Console

Define target device personality for multiple devices:

1. In the Console, right-click on the target device that has the personality settings that you want to share with other device, then select Copy. The Copy device properties dialog appears.
2. Highlight the target devices in the details pane that you want to copy personality settings 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 virtual disk 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
<!--NeedCopy-->
```

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 virtual disk 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>
<!--NeedCopy-->
```

The xx is the name of the disk. A virtual disk name cannot start with a $. This symbol is used for reserved values such as $DiskName and $WriteCacheType. The following message displays if a name that starts with $ is entered:

```
A name cannot start with a $. This is used for reserve values like
    $DiskName and $WriteCacheType. The $DiskName and $WriteCacheType
    values can be retrieved on the target device using GetPersonality.
    exe.
<!--NeedCopy-->
```

The `$WriteCacheType` parameter includes the following options for **RAM Cache with overflow to local hard disk** mode:

- private = 0
- serverCache = 1
- deviceRamCache = 3
- deviceDiskCache = 4
- deviceRamDisk = 6
- serverPersistent = 7
- deviceRamCacheWithDiskOverflow = 9 *

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:

“‘ pre codeblock
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.

1.  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
    <!--NeedCopy-->
```

```
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
<!--NeedCopy--> ```

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.
```

Configuring target devices that use personal vDisks

December 28, 2018

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 Provisioning Services farm, the wizard creates and adds target devices with personal vDisks to an existing site's collection. The wizard assigns an existing shared-mode vDisk to that device.

The wizard also creates virtual machines to associate with each device. A catalog in Citrix Desktop Studio 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. Including application settings, adds, deletes, modifications, documents.

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

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

General tab

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

- 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 port), you must change this value.

- 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

- 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

- Target Device Status

The following target device status information appears:

- Status: 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

- 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 — 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 vDisks 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 compatibility with your actual environment.

Considerations

- Personal vDisk devices can be test or production devices.
- Provisioning Services 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 Provisioning Services console with these methods:
  - Change assignment with Target Device properties vDisk tab. For more information, see Target Device Properties.
  - Copy and paste target device properties. For more information, see 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 more privileges for the soap/stream services user.
  - Local administrator on the Provisioning Services server system.
  - XenDesktop full administrator.
  - Full permission to the XenDesktop database (a XenDesktop requirement).
- For merging, Provisioning Services 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 might potentially interfere with merging.
- By default, Studio does not show the personal vDisk stage. 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, change it to *test*. 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.

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, except 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.

About the common vDisk image feature

December 28, 2018

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 Create Common Images for use with XenServer VMs and Physical Devices, or Blade Servers.
- 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 Create Common Images for use with XenServer VMs and Physical Devices, or Blade Servers

Create common images for use with XenServer VMs and physical devices, or blade servers

December 28, 2018

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 Provisioning Services 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 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 very 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 and add a new NIC.
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 master target device.
8. Verify that Provisioning Services successfully bound to the XenServer NIC and the physical systems NIC.

Image the Provisioning Server master target device

Use either the Provisioning Services 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 Provisioning Services 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 Provisioning Services 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 steps that follow.

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 (installs all drivers).
   c) Install all necessary Windows updates.
   d) Install Provisioning Services 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 Provisioning Services 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.

Prerequisites for deploying vDisks

December 28, 2018

vDisks are configured before being deployed. Configuration tasks include:

- Selecting the vDisk Access Mode and if applicable, the Write Cache Mode for that vDisk, see Configuring the vDisk Access Mode. And 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 (for details, refer to Enabling Domain Management.
- 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.
  - Providing vDisk identification information (for details, refer to Identification information in the vDisk Properties.

Configuring the vDisk access mode

December 28, 2018

Use the Console to select from the following vDisk access modes:

- Standard Image –Select this mode if a vDisk is shared by multiple target devices (write-cache options enabled).
- Private Image –Select this mode if a vDisk is only used by a single target device (read/write access is enabled).

Standard Image mode

Standard Image mode allows multiple target devices to stream from a single vDisk image at the same time. This mode reduces the amount of vDisk management and reduces storage requirements.

When a vDisk is configured to use Standard Image mode, it is set to read-only mode. Each target device then builds a write cache to store any writes the operating system needs to make. There are several write-cache options available. Because the vDisk is read-only, each time a target device boots, it always boots from a 'clean'vDisk. If a machine becomes infected with a virus or spyware, the target device only needs to reboot the image.

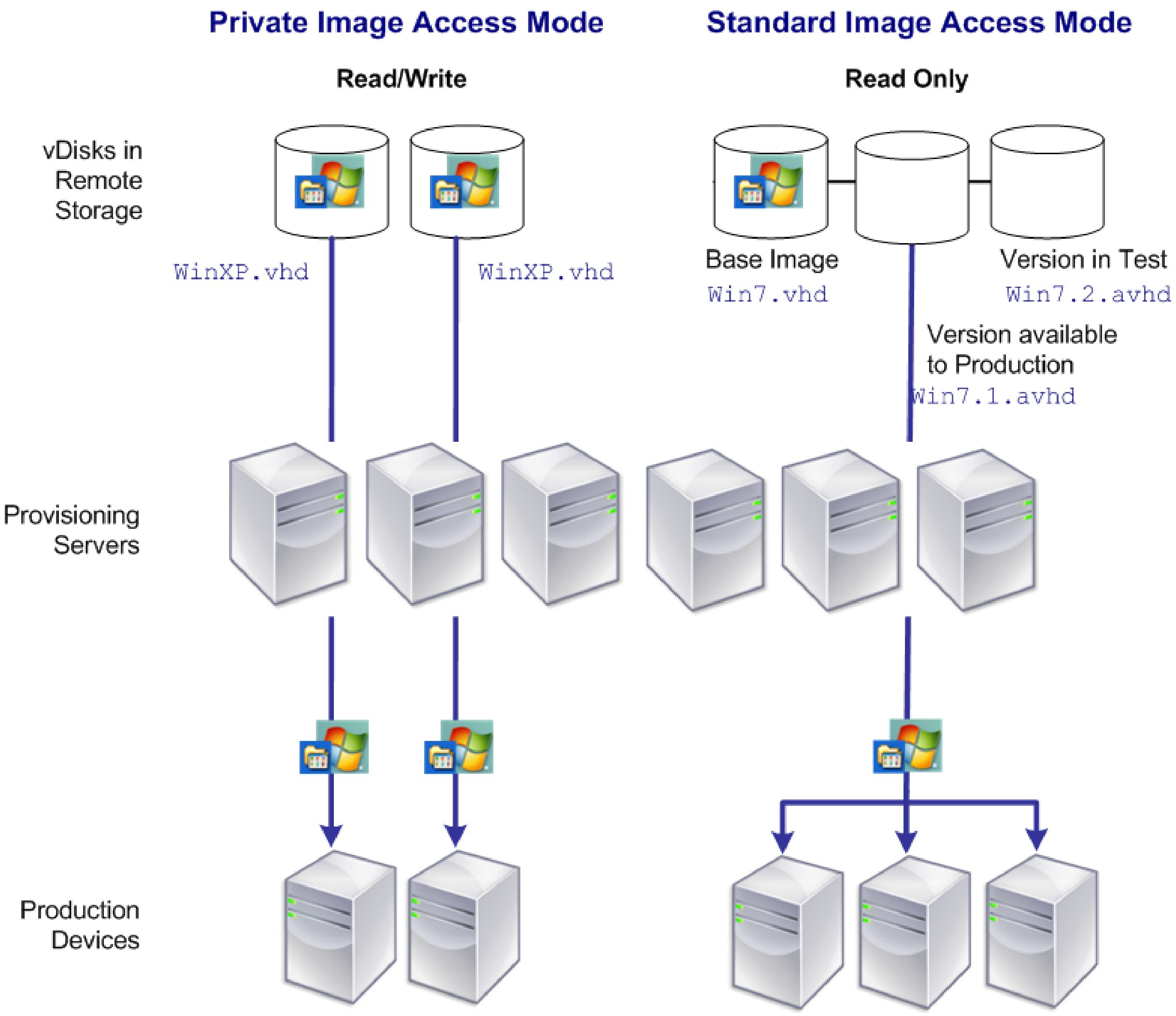
When updates are made to a vDisk in Standard Image mode, changes against the base vDisk image are captured in a differencing disk file (.Avhdx), resulting in a new version of the base image. Each new version remains directly associated with the base image. Versioning allows for the updates captured in the differencing disk to be staged (Maintenance, Test, Production) before those changes become available to Production devices. If issues are encountered with a version, that version can simply be reverted. For details on versioning, refer to Updating vDisks.

Although each target device uses the same vDisk, Provisioning Services personalizes the streamed image for each target device. PVS provides the information needed to ensure the device is uniquely identifiable on the network. You can also specify more personality settings for each device: you can store application-specific values in the database and retrieve the target device's unique value as the device loads. For more details, refer to Managing Target Device Personality.

Private image mode

A vDisk that is in Private Image mode closely models how a computer uses a regular hard drive. That is, only one target device can use a Private Image vDisk at a time.

The following illustrates Private Image vDisks (read/write) that are each assigned to a single production device. The image also shows a Standard Image vDisk (read-only) that is assigned to and shared by a collection of production devices. For Standard Image vDisks, write cache options include cache on server disk, on a device's hard disk drive, or in the device's RAM.



To configure the vDisk mode and any applicable write cache destination

Note: Only write cache destinations that are supported for Standard access mode appear enabled.

1. On the Console, right-click on the vDisk for which you want to configure the vDisk access mode, then select **vDisk Properties**. The **vDisk Properties** dialog appears.
2. Click the **General** tab, then select the image mode (Standard or Private) that applies to this vDisk from the **Access Mode** drop-down list.
3. If Standard image was selected, from the cache destination drop-down list, select the appropriate write cache destination.
4. Click **OK** to exit the **vDisk Properties** dialog.

Configuring a vDisk for Microsoft volume licensing

April 19, 2021

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

> **Note**
>
> The MCLI and SoapServer command-line interfaces can also be used to configure Microsoft volume licensing.

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 use of the Key Management Server (KMS) license keys with Provisioning Services.

Provisioning Services support for KMS licensing requires that the SOAP Server user account represents a domain user with the right to perform volume maintenance. 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 that runs in the datacenter. It serves as a local activation point (opposed to having each system activate with Microsoft over the internet).

> **Note**
>
> When preparing or updating a KMS configured vDisk that is copied or cloned, it is important to complete the final KMS configuration task. This task is to change the vDisk mode from **Private Image Mode** to **Shared Image Mode**, before copying or cloning the vDisk to other Provisioning Servers. Also, both the .pvp and .vhdx file must be copied 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 Provisioning Services farm include:

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

If KMS licensing was not configured on the vDisk when the Imaging Wizard was run, it can alternatively be configured using the Console user interface. Refer to the **Microsoft Volume Licensing** tab, or the MCLI and PowerShell command-line interfaces. Refer to the MCLI or PowerShell Programmers Guide for details.

Preparing the new base vDisk image for KMS volume licensing

After a vDisk is created using the Imaging Wizard, it must be reset to a non-activated state using the rearm command. For additional information about this command, see Configuring KMS Licensing for Windows and Office.

It is important to 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.

> **Note**
>
> Microsoft limits the number of times you can run rearm on an installed OS image. Reinstall the operating system if the number of allowed rearm attempts is exceeded.

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 vDisk has gone through base disk preparation once, repeat base disk preparation:

   a) In the Console, right-click on the vDisk, then select the **File Properties** menu option. The vDisk File Properties dialog appears.
   b) Click on 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 on the vDisk, then select the **File Properties** menu option. The vDisk Properties dialog appears.
   g) Click on 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). This allows activation of systems that do not have network access to the internet. Provisioning Services applies this proxy activation mechanism for Standard Image mode vDisks that have MAK licensing mode selected when the vDisk is created.

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

Upon first execution of the VAMT, a VAMT database is created. This database caches all device activations and allows for Provisioning Services to reactivate.

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

Provisioning Service MAK activation requires configuration for three types of users.

- **Volume Activation Management Tool/Provisioning Services installation user** —This user is a local administrator on the Provisioning Services server system and has the rights on SQL 2012 or newer (VAMT 3.1 requirement) to create a database for VAMT to use.
- **MAK user** —This is the user set 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 Services server and the master client. This user requires full access to the VAMT database.
- **Provisioning Services 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 Services 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 Provisioning Services target devices.
4. If the user who created the VAMT database is not the soap/stream services user, copy the VAMT configuration file C:\Users\<VAMT installation user (dB creator)>\AppData\Roaming\Microsoft\VAMT\VAMT.co to C:\Users\<Provisioning Services soap/stream services user>\AppData\Roaming\Microsoft\VAMT\VAMT.con
5. Set the Provisioning Services server security configuration to use PowerShell to interface with VAMT.

   a) Set-ExecutionPolicy -Scope \ (the Provisioning Services services user) to *unrestricted* –see Set-ExecutionPolicy for more information.
   b) WinRM quickconfig.
   c) Enable-WSManCredSSP -Role Client -DelegateComputer <this server's fqdn> -Force
   d) Enable-WSManCredSSP -Role Server –Force.

6. Configure the Windows firewall on the client for VAMT 3.1 –see Configure Client Computers for more information. Citrix Provisioning target devices cannot be activated or reactivated if the firewall is not configured for VAMT.

Common activation errors

Error: Failed to create PSSession —Reason: MAK user is not a local administrator on the Provisioning Services 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's licensing mode for MAK

A vDisk can be configured to use Microsoft Multiple Activation Key (MAK) licensing when running the Imaging Wizard. Refer to Imaging Wizard. If MAK licensing was not configured when the Imaging Wizard was run, set the vDisk's licensing mode property 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.

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 and user credentials have been entered, each booted target device assigned to the vDisk needs to be activated with a MAK.

Note: After all licenses for a given MAK have been used, a new key will be required to allow more target devices that share this vDisk image to be activated.

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 that includes those target devices that require 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 be used 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 should be activated.

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 results 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. After the activation process completes, if one or more target devices were not selected to be activated, or if devices were not activated successfully, the dialog displays listing 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:

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

To update a MAK activated vDisk, the AutoUpdate feature must be used so that the MAK activation information, required for shared device reactivation, is maintained.

More MAK considerations:

- Use of manual vDisk updates (unassigning one vDisk and reassigning another vDisk) results in the loss of the required MAK activation information and requires a new activation, which would consume another license.
- Use of AutoUpdate 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 Provisioning Services console.

Managing load balancing across servers

December 28, 2018

A vDisk can be configured so that a single server provides that vDisk, or configured so that multiple servers can provide the vDisk using a load balancing algorithm.

To configure load balancing on a vDisk

1. Right-click on the vDisk in the Console, then select the **Load Balancing**…menu option.
2. Select to enable load balancing or to assign a single Provisioning Server to provide this vDisk, then click **OK**. Refer to the table below for dialog details.

Note: For details on configuring for high availability, refer to
Managing for Highly Available Implementations.

The following table describes the vDisk Load Balancing dialog.

Field	Description
Use the load balancing algorithm	Provides the option to enable or disable the load balancing algorithm, which selects the server that is least busy to provide this vDisk to target devices.
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. None is the default setting. Best Effort –use the least busy server/NIC combination from within the same subnet. If no server/NIC combination is available within the subnet, select the least busy server from outside the subnet. If more than one server is available within the selected subnet, perform load balancing between those servers. Fixed –use the least busy server/NIC combination from within the same subnet. Perform load balancing between servers within that subnet. If no server/NIC combination exists in the same subnet, do not boot target devices assigned to this vDisk.

Field	Description
Rebalance Enabled	Enter or edit a description for this farm. Enable to rebalance the number of target devices on each server when the trigger percent is exceeded. When enabled, Provisioning Services checks the trigger percent on each server every 10 minutes. **Note:** Rebalancing fails if there are less than five target devices on each server, or if more than 20% of the target devices are currently booting. A target device that is currently booting is not moved to a different server.
Trigger Percent	Percent The percent of overload that is required to trigger the rebalancing of target devices. For example: If the trigger percent is equal to 25%, rebalancing occurs if this server has 25% more load in comparison to other servers that can provide this vDisk. Values between 5–5000. Default is 25.
Use this server to provide the vDisk	To assign a specific server to provide this vDisk, enable the Use this server to provide the vDisk radio button.

Assigning vDisks and versions to target devices

December 28, 2018

This document tells you how vDisk version access modes relate to target device types, and how to assign and unassign a vDisk to a target device, and

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 promoted from Maintenance to Test and then into Production. Access mode options include:

Maintenance –new read/write difference disk version that is only available to the first Maintenance device that selects to boots from it to make updates.

Test –read-only version used for test purposes and only available to Test or Maintenance devices.

Pending –read-only version and not yet available for use by Production devices because the scheduled release date and time have 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 updated a vDisk manually. To do this, a new version is requested from the vDisk Versions Dialog, which creates a 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. For additional information on merging vDisks, refer to Merging VHDX Differencing Disks.

- 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 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 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 Devices or Unassign from All Site Devices menu option.

2. If unassigning from select devices, in the Unassign from Devices dialog, select the devices to unassign to this vDisk, then click **Unassign**. If unassigning from all devices in a site, click **Yes** on the confirmation dialog that appears.
3. After the target devices are successfully unassigned, close any open dialogs.

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 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. Date format is YYYY/MM/DD and time format is HH:MM.

- Devices

The number of target devices streaming sessions for a given version.

- Access

Indicates target device access availability for a given version.

Maintenance read/write version that is available to the first maintenance device that selects to boots from it.

Test read-only version used for test purposes and only available to test or maintenance devices.

Pending read-only and not yet available for use because the scheduled release date and time have not been reached.

Default read-only version that is bootable by all devices. If the Boot production devices from version is set to Newest released, 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 this version was released to production.

- Type

Identifies how the vDisk was created. The options include:

```
-  Manual - created using Maintenance mode.

-  Automatic - created automatically using an automated update.

-  Merge - created by a partial merge operation.

-  Merge Base - created by a base merge operation (no parent needed).

-  Base - the original base image.
```

- New

Creates a maintenance version.

- Promote

Opens a dialog that prompts to promote this version to Test or Production. If Production is selected, a release date and time can be set or the default (now) can be accepted.

- Revert

Reverting from Test version: if no maintenance access version exists, revert moves latest test version into Maintenance.

Reverting from Production: any booted device is shut down before reverting. Clicking **Revert** opens a dialog that allows the user to select to revert to Test or Maintenance.

- Delete

Clicking **Delete** opens a delete confirmation dialog. Click **OK** to delete the selected version. Delete is only available if the latest version or obsolete version doesn't have target devices currently booted from it.

- Replication

Selecting a version, then clicking Replication opens the **Disk Versioning Replication Status** dialog. This dialog displays the replication status of this version on each server:

- Blue check next to the server name indicates that the version has been replicated on the server.
- Orange triangle next to the server name indicates that the version has not yet been replicated or there is an issue. Placing the cursor over the triangle displays the related error message.

To view the replication status of all versions of this vDisk on each server, right-click on the vDisk in the Console, then select **Replication Status** from the context menu.

- Properties

Clicking the **Properties** button opens the vDisk Version Properties dialog, which allows you to enter a description related to this version. It also displays availability of a selected version if that version is set for release to production in the future, or if no device has booted from that version yet.

- Text

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

Updating vDisks

November 6, 2019

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) to capture the changes without changing the base vDisk image.

Updating a vDisk involves the following:

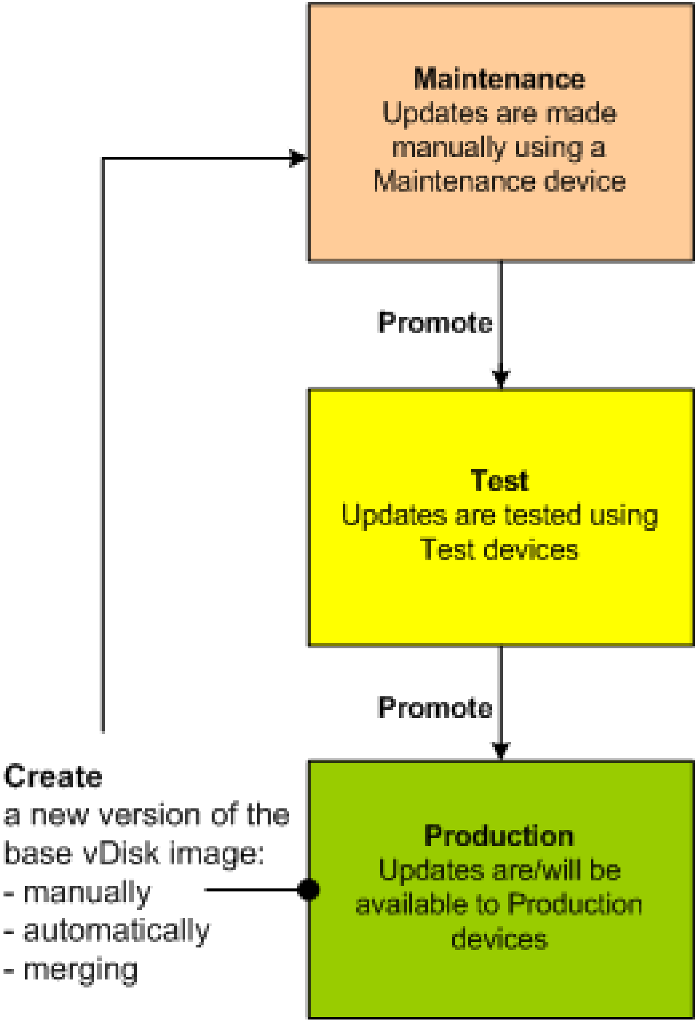
- Create a version of the vDisk, manually or automatically.

- 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.

There are three ways to update a vDisk:

- boot in private image mode
- versioning
- reverse imaging

The following illustrates the general promotion of a vDisk update:


Maintenance
Updates are made manually using a Maintenance device
Promote
Test
Updates are tested using Test devices
Promote
Production
Updates are/will be available to Production devices
Create
a new version of the base vDisk image:
- manually
- automatically
- merging

The availability of the updated version depends on the current promotion of that version (maintenance, test, or production). Availability is also determined by the type of device attempting to access it (Maintenance Device, Update Device, Test Device, or Production Device).

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

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.

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 then verify updates were made.
5. Promote the test version to production.

Update scenarios

The following vDisk update scenarios are supported:

- **Manual Update** –An administrator can update a vDisk manually by creating a version of that vDisk, and then using a Maintenance device to capture updates to that version. Manual updates are initiated by selecting the **New** button on the vDisk Versions dialog. The **Access** column on the vDisk Versioning dialog displays that the newly created version is under maintenance. While under maintenance, this version can only be accessed and 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. For details, refer to Manually Updating a vDisk Image
- **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 displays that the newly created version is under maintenance. While under maintenance, this version can only be accessed and updated by the one Update device to which it is assigned (only one Update Device exists per vDisk). For details, refer to Automating vDisk Updates.
  Note: vDisk Update Management is intended for use with Standard Image Mode vDisks only. Private Image Mode vDisks can be updated using normal software distribution tool procedures. Registering a Private Image Mode vDisk for Update Management, or switching a vDisk that is already registered, causes errors to occur.
- **Merge** –Merging VHDX differencing disk files can save disk space and increase performance, depending on the merge option selected. Manually merge an update 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

December 28, 2018

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 that base disk.

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, as captured in the table that follows.

	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

For information on merging VHDX files, refer to merging VHDX files.

Manually updating a vDisk image

June 3, 2019

The vDisk Versions dialog allows you to manually create a version of the vDisk's base image.

Note: To automate an update process, configure for vDisk Update Management. See Automating vDisk Updates.

This procedure requires that:

- a Maintenance device has been assigned to the vDisk being updated.
- no version of this vDisk is under maintenance.
- no active/booted target device in maintenance or test mode can be promoted.

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.

To 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: If booting a Test or Maintenance device, a boot menu displays that allows the user to select from which vDisk, or version of that vDisk, to boot from unless the device is a PvD Test device.
   Important: You cannot promote an active/booted target device in maintenance or test mode. If an active target device exists on the promoted version, the console displays an error stating `Error Active Device. The task cannot be performed on active devices. Shut down the devices before attempting to perform this task.`
4. Right-click on the vDisk, then 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.

Automating vDisk updates

December 28, 2018

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 Private Image Mode vDisk for vDisk Update Management, or switching a vdisk that is already registered, causes errors to occur.

In the Console, the vDisk Update Management feature is used to configure the automation of vDisk updates using virtual machines (VMs). Automated vDisk updates can 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

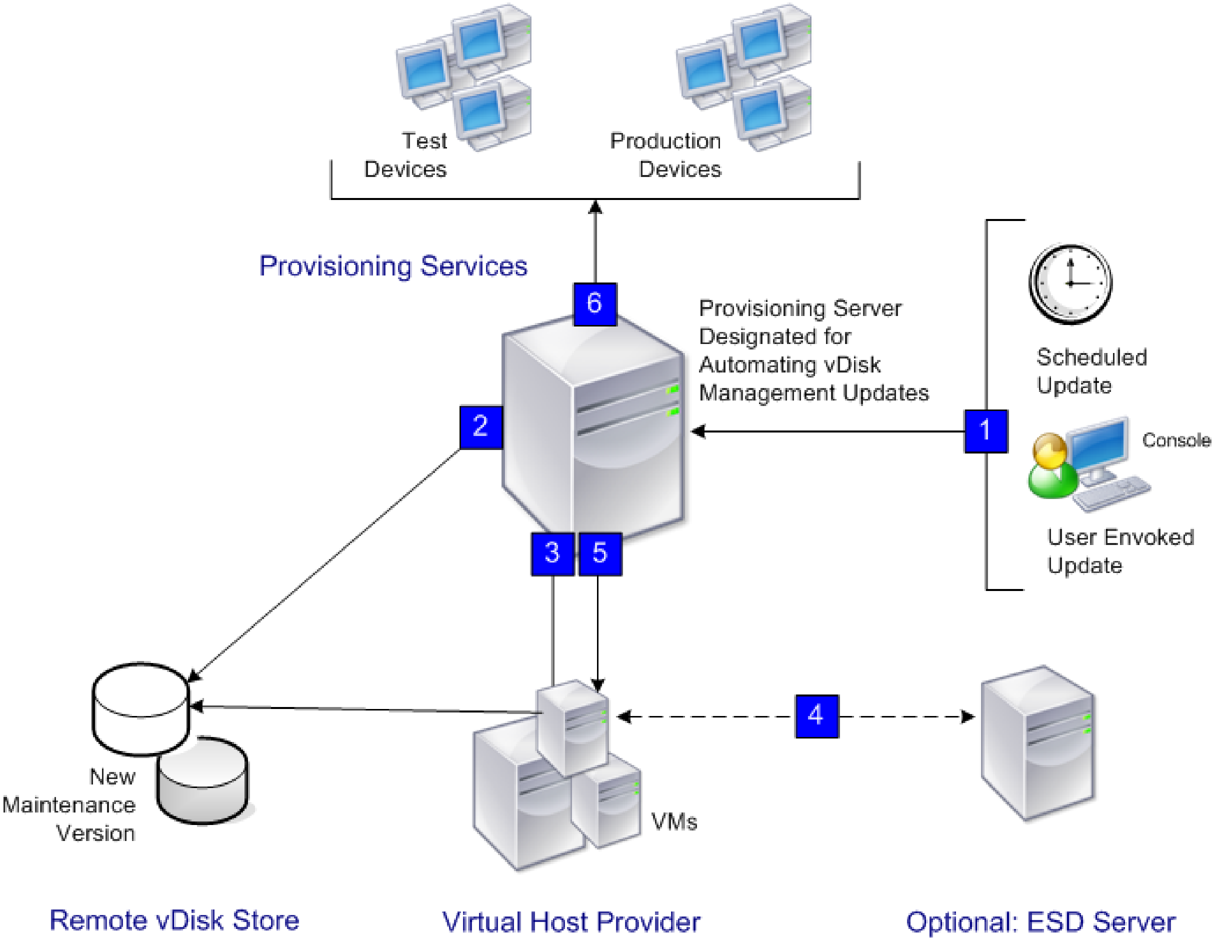
To configure a site for vDisk Update Management requires completing the following high-level tasks:

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 to update the vDisk. Refer to Creating and configuring ESD update VMs.
4. Configuring vDisks for Automated updates.
5. Creating and managing update tasks. Refer to Create and manage tasks.
   Note: The user that configures vDisk Update Management tasks must have permissions to create, modify, and delete Active Directory accounts.
6. Run the update task by right-clicking on the task object in the Console, and then selecting the **Run update now** menu option. The Update VM boots, install updates, and reboot as necessary. After the update task successfully completes, the virtual machine is automatically shut down. The update status can be checked from the Console tree under vDisk ****Update Management\ > vDisks>(****vDisk name)> Completed Update Status. The status can also be checked using the event viewer or in WSUS.

After the site is configured to use vDisk Update Management, managed vDisks can be updated using the following methods:

- **Scheduled** –the Image Update Service automatically updates a vDisk, on a scheduled basis as defined in the Update Task. For more details, refer to Create and manage tasks or Update task properties.
- **User Envoked** –select a managed vDisk from the **Consoles Run update now** menu option. This option requires that the administrator manually start, then stop the Update Device after the update is complete.

The following illustrates the basic update process for both scheduled or user invoked update methods:



1. 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.
2. Provisioning Services creates a version (VHDX) and places that version in Maintenance mode (read/write).
3. The virtual machine boots the assigned vDisk:
   - Scheduled update –vDisk Update Management performs the boot automatically.
   - User invoked update –the administrator invokes the update.
4. All updates are automatically made and captured in the new version of the VHDX file.

5. After you update the vDisk, the virtual machine is shut down automatically.
6. 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, the mode that is currently 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

December 28, 2018

To automatically update Managed vDisks:

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. Scroll to 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

June 3, 2021

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://{ 0 } :PORT#/sdk`. If you are using port 300, `ServerConnectionString= http://{ 0 } :300/sdk`.

To configure virtual host connections:

1. Under the vDisk Update Management node in the 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.

Field	Description
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://{ 0 } :PORT#/sdk`. If you are using port 300, `ServerConnectionString= http://{ 0 } :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.
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.

Creating and configuring ESD update VMs

December 28, 2018

Virtual machines (VMs) that are used to update a Managed vDisk are first created on the hypervisor before configuring for vDisk Update Management in Provisioning Services. Supported hypervisors include: Citrix Xenserver, Microsoft SCVMM/Hyper-V, and VMWare vSphere/ESX.

The type of ESD determines the specific steps involved in creating and configuring the VM on the hypervisor. However the following general prerequisites apply to Update VMs regardless of the ESD system selected:

- Download, install, and configure the appropriate ESD Server software on the server.
- A VM must be uniquely named on the hypervisor and follow naming conventions equivalent to a Provisioning Services target device name. The name can be up to 15 bytes in length.
- Only one VM should exist for a Managed vDisk because only one update task can occur on that vDisk at any given time.
- Citrix recommends allocating at least 2GBs of memory for each VM.
- Appropriate ESD licenses must be made available and the ESD client software must be properly installed and enabled on the vDisk.

- Using Microsoft HyperV Server without SCVMM is not supported.
- Configuring the Update VM, that is used to build the Update vdisk, with multiple NICS when streaming to SCVMM server fails to PXE boot. Citrix suggests using a single NIC or use only one Legacy NIC.
- Because the image update client requires .NET 3.5 or higher, it must be installed on the vDisk that serves the update VM.
- Citrix recommends to only apply updates that can be downloaded and installed in 30 minutes or less.

The following ESD systems are supported:

- WSUS
- SCCM

Configuring managed vDisks for automated updates

December 28, 2018

vDisk Update Management uses virtual machines to process updates to managed vDisk(s). vDisks are first created in the
Console, then added to vDisk Update Manager as managed vDisks by running the Managed vDisk Setup Wizard.

Note: If using ESD Servers to deliver updates, the ESD client software must be installed and enabled on the vDisk, and appropriate ESD licensing must also be available.

1. Under the vDisk Update Management node in the Console tree, right-click on vDisks, then select the **Add vDisks…** option. The Managed vDisk Setup Wizard Welcome page appears.
2. Click **Next** to begin. The **vDisk page** appears.
3. Select the default search options (All stores, All servers). Or, use the filtering options to select specific stores and/or servers to display the vDisk(s) to select to be managed. vDisks that are not already managed appear in the vDisk selection box.
4. Select one or more vDisks to be managed, then click **Next**. The Host/VM page appears.
5. Select the type of connection to use when hosting the VM, from the appropriate drop-down list.
6. Enter the name of the Update VM used to process the vDisk update. The **VM name** field is case sensitive and must match exactly to the existing VM name on the desired hypervisor.
7. Click **Next**. The Active Directory page appears.
8. If you are using Active Directory, enter a Domain and Organizational Unit to create an Active Directory machine account. This account is used by the Update Device that is created exclusively for updating this vDisk, then click **Next**. The **Confirmation** page appears.

Note: The Update VM should not already pre-exist in the Provisioning Services database or Active Directory. If it does exist, the wizard fails to run.

1. Review all setting, then click **Finish**.

The Managed vDisk Setup Wizard can also be run from the Managed vDisk dialog, which displays all Managed vDisks
currently in the store. The Managed vDisk Setup Wizard can be run from the Managed vDisk Dialog by clicking the Add Managed vDisks button.

Creating and managing tasks

December 20, 2018

Note: The user that configures vDisk Update Management tasks must have permissions to create, modify, and delete Active Directory accounts.

Use the **Update Task Wizard** to schedule vDisk updates to run automatically:

1. Under the **vDisk Update Management** node in the Console tree, right-click on Task, then select the **Add task…** menu option. The Update Task Wizard welcome page appears.
2. Click **Next** to begin configuring a task. The Name/Description page appears.
3. Enter a name (required) to identify this task, and a description (optional) in the appropriate text boxes, then click **Next**. The Schedule page appears.
4. Select one of the radio buttons to determine how often this task runs; None, Daily, Weekly, or Monthly. Depending on which recurrence option was selected, the page displays options specific to that selection:

- None –no additional options appear.
- Daily
  - Run the update at –select the time of day to run the daily update from the drop-down menu or enter a specific time.
  - Everyday –select to run this daily update everyday of the week: Monday through Sunday.
  - Weekdays only –select to run this daily update on weekdays only: Monday through Friday.
- Weekly
  - Run the update at –select the time of day to run the daily update from the drop-down menu or enter a specific time.
  - Select specific days of the week to run the update.

Note: At least one day must be selected to proceed.

- Monthly
  - Run the update at –select the time of day to run the daily update from the drop-down menu or enter a specific time.
  - Select to run the update task on specific days of the month using one of the following methods: On Date –enter which days of the month to run the update.

Note: Only numbers and commas are accepted in this text box. For example: 1,15 runs this update task on the first
and fifteenth of every month. If either 29 or 31 are entered, this task does not run every month. Or, select **On**, to select the week and day of the week from the drop-down menus. For example: Selecting First and
Monday would run the task on the first Monday of every month.

1. Click **Next**. The vDisks page appears.
2. Highlight existing Managed vDisks that updated using this new task, then click **OK**. Optionally, click on the Add Managed vDisks button run the Managed vDisk Setup Wizard to add new managed vDisks to the list. After the wizard completes, the new managed vDisks display in the list and can be selected.
3. Click **Next**. The ESD Client page appears.
4. Select the type of Electronic Software Delivery (ESD) client that is running on the vDisk, from the drop-down list, then click **Next**.

Note: The ESD client software should be installed in the vDisk image. When the option is set to None, client-side scripts can be run if the scripts are stored on the vDisk before the update. These scripts need to be stored under the installation directory of the client. Update.bat is a mandatory script. Optional scripts include **Preupdate.bat** and **Postupdate.bat**, which are dependent on the users configuration.

1. Optionally, select from the following scripting options, then click **Next**:

- Pre-update script –executes before the start of any update task process.
- Pre-startup script –executes just before startup of the virtual machine.
- Post-shutdown script –executes just after the virtual machine shuts down.
- Post update script –executes after the update task process completes.

Note: On the server, a subfolder named **Scripts** must be created under the product installation directory. This folder is used to store server-side scripts.

1. On the vDisk Access page, select the post-update access mode to assign to the vDisk version, then click **Next**:

- Leave the vDisk in Maintenance mode (only available to Maintenance Devices)
- Place the vDisk in Test mode (only available to T est and Maintenance Devices)

- Make the vDisk ready for use (Production, available to all target devices)

1. Confirm that all vDisk Update T ask settings are correct, then click **Finish** to create the task. vDisk Update Tasks can be viewed and modified on the **Update Task Properties** dialog.

Using Windows Task Scheduler to create vDisk update task scripts

December 28, 2018

Windows Task Scheduler can be used to create vDisk Update task scripts. These scripts are associated with a task when the Update Task Wizard is run. They can be modified later on the **Scripts** tab of the **vDisk Update Task Properties** dialog.

Note: Features of the Task Scheduler are used to run the batch file/script as the desired user.

The following types of task scripts can be created:

- Pre-update script - executes before the start of any update task process.
- Pre-startup script - executes just before starting the virtual machine.
- Post-shutdown script - executes just after the virtual machine shuts down.
- Post update script - executes after the update task process completes.

Scripts are stored in a Scripts folder, which is a subfolder of the product installation folder.

A sample batch file to boot target devices:

```
Mcli SetupConnection /p server=192.168.1.1
Mcli Run Boot /p deviceMac=00-00-00-00-00-11
Mcli SetupConnection /p server=192.168.1.1
Mcli Run Boot /p deviceMac=00-00-00-00-00-11
Mcli Run Boot /p deviceMac=00-00-00-00-00-22
Mcli Run Boot /p deviceMac=00-00-00-00-00-33
Mcli Run Boot /p deviceMac=00-00-00-00-00-44
Mcli Run Boot /p siteName=Boston collectionName=Sales
```

A sample batch file to check for vDisk updates:

```
Mcli SetupConnection /p server=192.168.1.1
Mcli Run ApplyAutoUpdate /p siteName=Boston
```

Note: When configuring the server connection using the **Mcli-Run SetupConnection** command, do not specify the user, password, or domain. These values are not protected in the batch file/script.

Updating vDisks on demand

December 28, 2018

To make an unscheduled update to a Managed vDisk:

- Under the vDisk Update Management node in the Console tree, right-click on a Managed vDisk, then select **Run update now** menu option. If the vDisk is included in more than one task, a dialog displays the tasks from which you can choose.
- Updating on demand requires that you manually start the Update Device, and then wait until it completes the update successfully.

Updating device properties

December 20, 2018

To view or modify Update Device properties, right-click on the device in the Console, then select the **Properties** menu option. Properties include:

- vDisk. Displays the vDisk that is assigned to this Update device. This field cannot be modified. Each Managed Device has a one-time relationship with a single vDisk of the same name.
- Virtual Host Connection. Displays the name of the virtual host server assigned to this device. This field cannot be modified.
- VM Name. The name of the virtual machine on the virtual host provider. This field cannot be modified.
- VM MAC. The media access control (MAC) address of the network interface card that is installed in the Update device. This field cannot be modified.
- VM Port. Provides the UDP port value. In most instances, the port number does not have to be modified. However, if Update device software conflicts with any other IP/UDP software (that is, they are sharing port), this value must be changed.
- 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 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. On this tab, a new personality string can be created, or an existing string modified or removed.

- Status. The following device status information appears:
  - Update Status: displays the status of the update as either inactive or active (update in progress).
  - Status: status of the 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'.
  - License information. Depending on the device vendor, displays product licensing information (including; n/a Desktop License, Datacenter License, XenApp License, or XenDesktop License).
- Logging level. Select the logging level or select **Off** to disable logging:
  - Off. Logging is disabled for this Provisioning Server.
  - Fatal. Log information about an operation that the system could not recover from. Error logs information about an operation that produces an error condition.
  - Warning. Log 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 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.

Merging VHDX differencing disks

April 14, 2023

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, which is given the file extension of .VHDX. This method allows for the fastest disk access to the base image and is recommended when performance is more important than disk space (a new base disk is created for every merge performed).

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 and 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.

An automatic consolidation of differencing disks can be configured from 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 and the availability of that virtual disk depends on the mode selected on the tab (Production, Maintenance, or Test).

Note: A consolidated differencing disk merge is recommended when disk storage is limited or when the bandwidth between remote locations is limited, which makes 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 fully 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. The Type column displays either Merge Base if a full merge was selected, or Merge if a partial merge was selected.

Promoting updated versions

September 20, 2019

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 updates are complete, this version can be promoted from Maintenance to Test (read-only) to allow for testing by test devices, or directly to Production, for use by all target devices.

Note: See Manually updating a vDisk and Automatically updating a vDisk.

After completing 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 Production is selected, a release date and time can be set, or the default (Immediate) can be accepted.

After completing an update using the automated update method, vDisk Update Management, the new version is promoted according to the Post Update setting selected when the Update Task Wizard is run. After the automatic update completes, promotion can also be set using the vDisk Version dialog' s Promote button.

If issues exist, the new version can be reverted back from Test to Maintenance (if no active sessions exist), or from Production to either Test or Maintenance (any booted device must be shut down prior to reverting).

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 version is set to Newest released (status is Default) 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.

Importing target devices into a collection

January 13, 2020

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 `.csv` file, it can then be imported into a device collection.

> **Note:**
>
> The `.csv` text file can be created with a `.txt` file, NotePad.exe, or Excel. It contains one line per target device, which is formatted as:
>
> `DeviceName,MAC-Address,SiteName,CollectionName,Description,Type`
>
> Where:
>
> ```
> DeviceName = Name of new target device MAC-Address = MAC address
>  of new device; such as 001122334455, 00-11-22-33-44-55, or
> 00:11:22:33:44:55 Type = 0 for production, 1 for test, or 2 for
>  maintenance
> ```

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 exist. There is also the option to use the default collection's device template, if it exists for that collection.

A log file is generated with an audit trail of the import actions. For Windows Server 2008 R2, the file is located in:

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

All other Windows Server operating systems generate the log file in `C:\ProgramData`.

To import target devices into a collection:

1. In the console, right-click on the device collection, then click **Target Device>Import devices**. The **Import Target Devices Wizard** displays.
2. Type or browse for the file to import. The target device information is read from the file and displays in the table. Information can include the target device name, MAC address, and optionally description.
3. Highlight one or more target devices to import. If applying the collection template to the imported target devices, select the **Apply collection template device** when creating devices check box.
4. Click **Import** to import the .csv text file containing target device information, into the selected collection. The status column indicates if the import was successful.

Managing views

December 28, 2018

The Console's Views feature 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 (Your Site).

To display or edit a views property, right-click on an existing view in the Console, then select the **Properties** menu option. The **View Properties** dialog displays and allows you to view or make modifications.

To perform actions on all members of a view, such as rebooting all target devices members in this view, refer to Configuring Views in the Console.

View properties

December 28, 2018

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/Button	Description
Name	The name given to this view.
Description	Describes the purpose of this view.

Members tab

Field/Button	Description
Members of this view	Lists target device members that belong to this view.
Add button	Opens the **Select Devices** dialog, from which target devices to add to this view are selected.
Remove button	Removes highlighted target devices from this view.
Remove All button	Removes all target devices from this view.

Managing for highly available implementations

December 28, 2018

Establishing a highly available network includes 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

Provisioning Services 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 Load Balancing Across 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

Database mirroring

November 19, 2020

In order to provide a highly available configuration, if you mirror a MS SQL database and the primary version becomes unavailable, Provisioning Services supports the mirrored version. This results in improved overall availability of Provisioning Services.

Database mirroring can be implemented in a new or existing farm and requires the following high-level tasks:

- Creating the Provisioning Services MS SQL primary database (created when the Installation Wizard is run 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 the Configuration Wizard is run).
- Identifying an existing MS SQL failover database server (identified, not created, when the Configuration Wizard is run).
- Configuring mirroring between the primary and failover database servers (configured using MS SQL database server tools)

Citrix recommends that you start the failover server before enabling database mirroring in the farm. For information, see Windows Server Failover Clustering with SQL Server.

Note:
The procedures that follow are only intended to call out the steps that are applicable to database mirroring when running the Configuration Wizard.

Note: Run the Configuration Wizard to specify the new failover server so that the status of the Provisioning Service's 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

To enable mirroring:

1. Start the Configuration Wizard on a server that will be 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 to use to communicate with this server.
6. Click Next. If the failover database has already been configured and it is up and running, Provisioning Services 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 Provisioning Services 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.

Provisioning Server failover

December 28, 2018

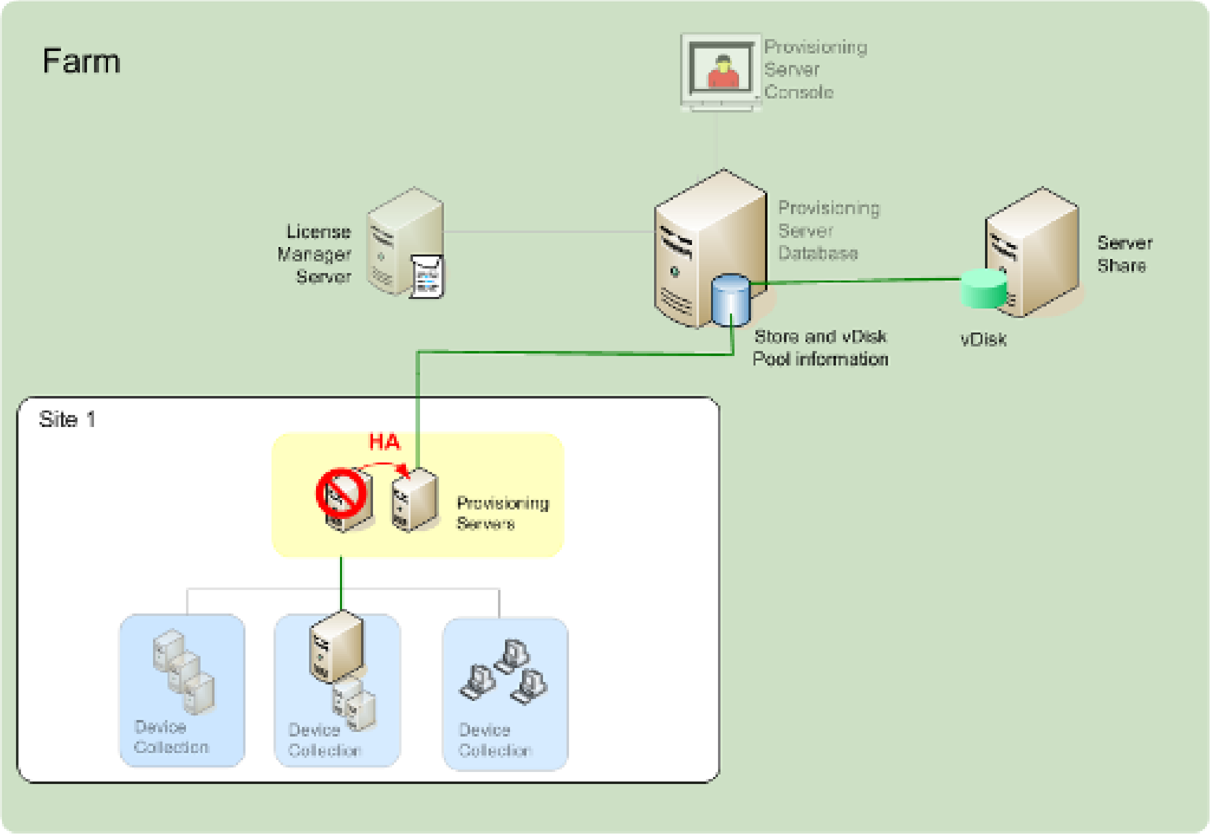
By default, all Provisioning Servers within a site that can access a vDisk can provide that vDisk to target devices. Multiple Provisioning Servers can access the same physical files on shared storage. This allows a target device to establish a connection on an alternate Provisioning Server if the connection to the active Provisioning Server is interrupted for any reason. A target device does not experience any disruption in service or loss of data when failover occurs.

Note: For implementations that use vDisk replication, if a server failover occurs, only those servers with access to an identical replicated vDisk can provide that vDisk to target devices. For example, if a vDisk is replicated across three servers hard drives and then 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 differs, therefore the vDisks are no longer identical.

Note: Provisioning Services does not support the high availability of vDisks on local storage that is in Private Image mode or that are currently in maintenance (read/write enabled).

If load balancing is enabled for the vDisk and a server providing that vDisk should fail, Provisioning Services automatically balances the target device load between the remaining servers. If the load balancing option is not enabled, a single server is assigned to provide the vDisk to target devices, therefore failover fails.

Note: For information on configuring Provisioning Services to automatically balance the target device load between servers, refer to
Balancing the Target Device Load on Provisioning Servers.



The Provisioning Server that a target device accesses to login does not necessarily become the Provisioning Server that accesses the vDisk on behalf of the target device. In addition, once connected, if one or more Provisioning Servers can access the vDisk for this target device, the server that is least busy is selected.

To purposely force all target devices to connect to a different Provisioning Server, while avoiding having targets timeout and attempt to reconnect to the current 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 and then 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 Provisioning Server changes to that of an alternate Provisioning Server in the vDisk status dialog on the target device.

Managing domain passwords

May 11, 2021

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.

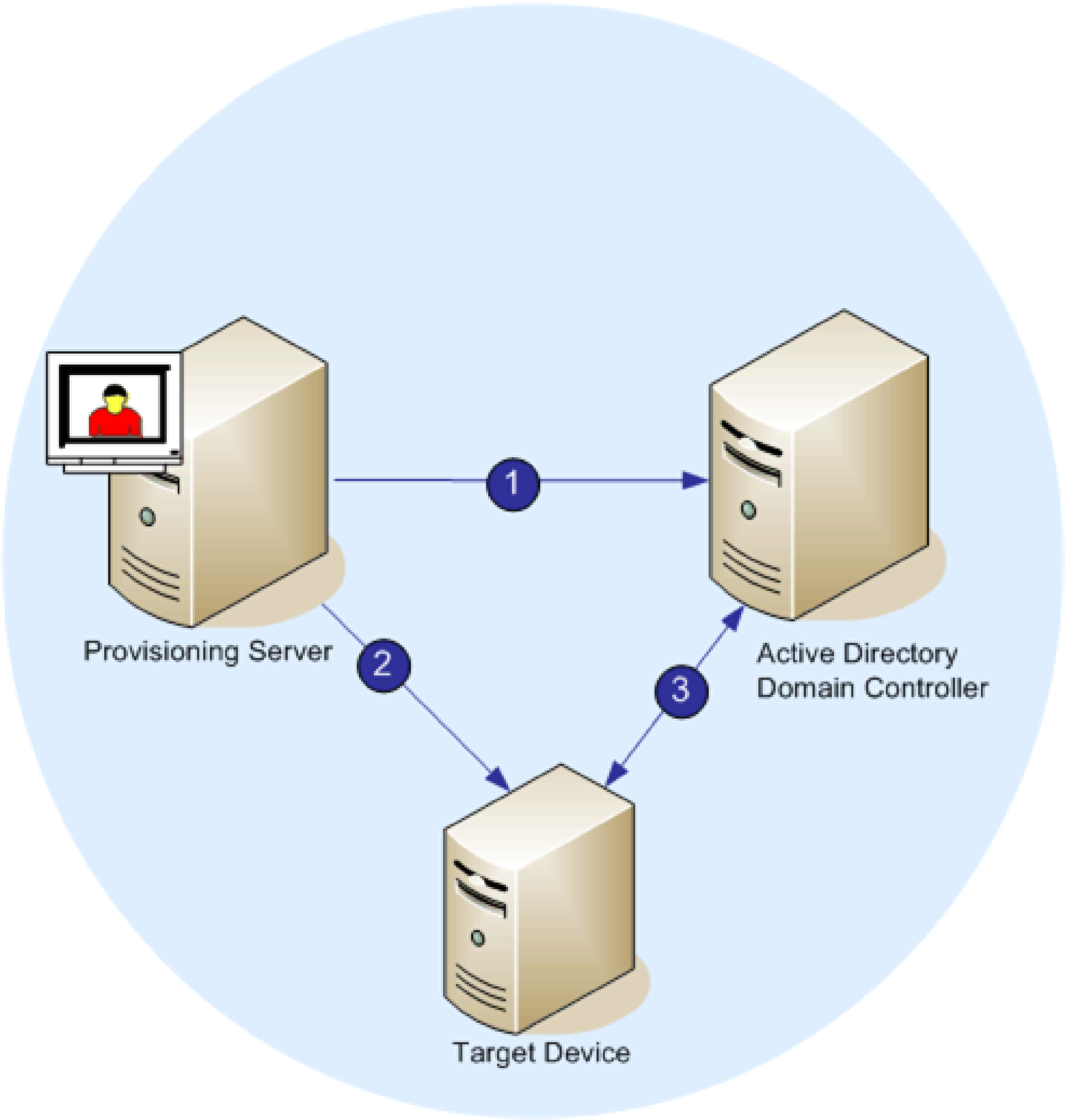
While target devices booting from vDisks no longer require Active Directory password renegotiation, configuring a policy to disable password changes at the domain level applies to any domain members booting from local hard drives. This may not be desirable. A better option is to disable machine account 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

May 11, 2021

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 the File 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 both 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

May 11, 2021

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.

Cross-forest configuration

This configuration is similar to the cross-domain scenario. However, in this configuration the Citrix Provisioning console, user, and administrator group are in a domain that is in a separate forest. The steps are the same as for the parent-child scenario, except that a forest trust must be established first.

> **Note:**
>
> Microsoft recommends that administrators do not delegate rights to the default Computers container. The best practice is to create accounts in the OUs.

Giving provisioning services administrator privileges to users from another domain

Citrix recommends the following method. For role-based administrators where the PVS is in one domain and the PVS administrator is in another domain, a two-way trust is required.

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 virtual disk image must not be used again within your environment.

1. Right-click on one or more target devices in the Console window. You can alternatively right-click on the device collection itself to add all target devices in this collection to a domain. Select **Active Directory**, then select **Create machine account**. The **Active Directory Management** dialog appears.
2. From the Domain scroll list, select the domain that the target device belongs to. Or, in the **Domain Controller** text box, type the name of the domain controller that the target devices are 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 are 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 to reset, then click the **Reset devices** button.

   > **Note:**
   >
   > Add this target device to your domain while preparing the first target device.

3. Click **Close** to exit the dialog.

4. Disable Windows Active Directory automatic password renegotiation. To disable automatic password renegotiation on your domain controller, enable the following group policy: Domain member: Disable machine account password changes.

   > **Note:**
   >
   > To make this security policy change, you must have sufficient permissions to add and change computer accounts in Active Directory. You have the option of disabling machine account password changes at the domain level or local level. If you disable machine

> account password changes at the domain level, the change applies to all members of the domain. If you change it at the local level (by changing the local security policy on a target device connected to the virtual disk in Private Image mode), the change applies only to the target devices using that virtual disk.

5. Boot each target device.

Preparing network switches

September 8, 2020

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

Note: For Provisioning Services 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

September 8, 2020

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 Provisioning Services, 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

September 8, 2020

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

Configuring 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.

Configuring 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.

Configuring 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:

Object	User Coniguration\Administrative Templates\Network\Offline Files
Policy	Disable user configuration of offline files
Setting	Enabled
Policy	Synchronize all offline files before logging off
Setting	Disabled
Policy	Prevent use of the Offline Files folder
Setting	Enabled

Configuring 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:

Object	Computer Configuration\Windows Settings\Event Log\Settings for Event Logs
Policy	Policy Maximum Application Log Size

Object	Computer Configuration\Windows Settings\Event Log\Settings for Event Logs
Setting	Relatively low value. Consider 512 kilobytes.
Policy	Maximum Security Log Size
Setting	Relatively low value. Consider 512 kilobyte.
Policy	Maximum System Log Size
Setting	Relatively low value. Consider 512 kilobytes.

Disabling 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 Provisioning Services 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 Provisioning Services 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

September 23, 2020

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\User profiles
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.

Configuring 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 to contain the redirected user folders:

   \\ServerName\ShareName

2. Give Full Control permission to everyone for the network share.

3. Enable Folder Redirection.

Object	Computer Configuration\Administrative Templates\System\Group Policy
Policy	Folder Redirection policy processing
Setting	Enabled

4. Redirect the Application Data folder.

Object	User Configuration\Windows Settings\Folder Redirection\Application Data
Properties	Basic or Advanced. Target folder location: \Server-Name\ShareName\%username%\Application Data

5. Redirect the Desktop folder.

Object	User Configuration\Windows Settings\Folder Redirection\Desktop
Properties	Basic or Advanced. Target folder location: \Server-Name\ShareName\%username%\Desktop

6. Redirect the My Documents folder.

Object	User Configuration\Windows Settings\Folder Redirection\My Documents
Properties	Basic or Advanced. Target folder location: \ServerName\ShareName\%username%\My Documents

7. Redirect the Start Menu folder.

Object	User Configuration\Windows Settings\Folder Redirection\Start Menu
Properties	Basic or Advanced. Target folder location: \ServerName\ShareName\%username%\Start Menu

Disabling 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:

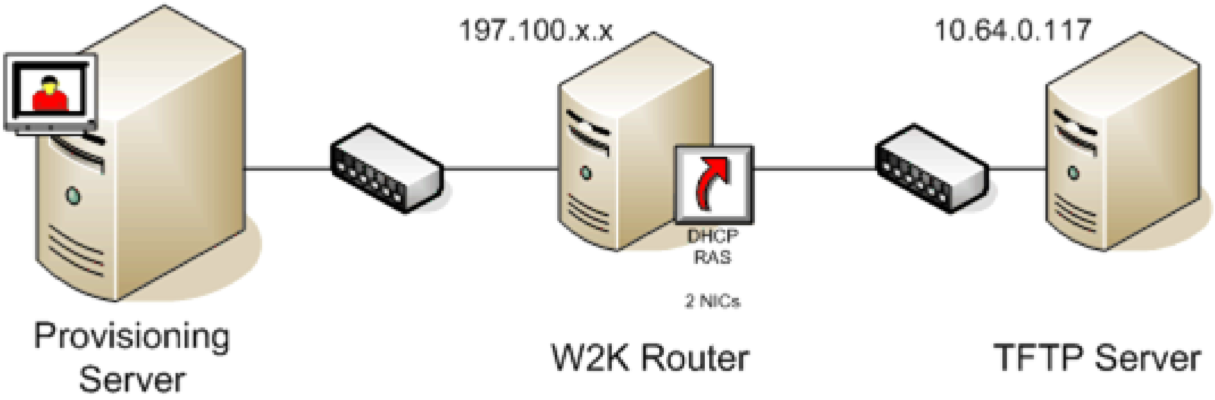
Object	User Configuration\Administrative Templates\Network\Offline Files
Policy	Disable user configuration of Offline Files
Setting	Enabled
Policy	Synchronize all Offline Files before logging off.
Setting	Disabled
Policy	Prevent user of Offline Files folder.
Setting	Enabled

Booting through a router

September 8, 2020

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.

Configuring the 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. Provisioning Services setup automatically adds this tag to your scope provided that the Microsoft DHCP server is installed and configured before installing 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.

```
pre codeblock 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; } . <!--NeedCopy-->
```

Managing multiple network interface cards

October 7, 2020

Provisioning Services 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, Provisioning Services overwrites the network configuration of the first NIC. All the other NICs'configurations are not changed. For a host with multiple network resources, Provisioning Services 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. Provisioning Services 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, Provisioning Services 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:

- Provisioning Services 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 Provisioning Services target device drivers.
- Teaming of multi-port network interfaces is not supported with Provisioning Services.
- Multi-NIC is supported for XenDesktop Private virtual machine desktops. Using the wizard, Provisioning Services 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.
- 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 Services 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 Provisioning Services installer automatically chooses the virtual NIC silently, without prompting.
- If changes are required, Provisioning Services 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 Provisioning Services 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 Services target device or Provisioning Server can be configured to support failover between multiple NICs. This feature works with any NIC brand or mixture of brands. Provisioning Services supports NIC failover for vDisks in either Standard and Private Image Mode.

- The PXE boot NIC is considered the primary target device MAC address, which is stored in the Provisioning Services database.
- You define the failover group of NICs when you run the Provisioning Services 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 Provisioning Services.
- 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 Provisioning Services 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, Provisioning Services 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.

Updating NIC drivers

June 7, 2021

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.

Upgrading NIC Drivers on Target Devices

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.

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.

Upgrading NIC Drivers on a Provisioning Server

To upgrade NIC drivers on any Provisioning Server, simply follow the manufacturer instructions for upgrading NIC drivers.

Managing printers

December 28, 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.

Do not use this feature 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

December 28, 2018

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 fails to 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, 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 (for details, refer to
enable printers for target devices.

Deploying virtual desktops to VMs using the XenDesktop Setup Wizard

June 14, 2022

Using a Provisioning Services streamed vDisk, the Provisioning Services XenDesktop Setup Wizard (XDSW) assists in deploying virtual desktops to virtual machines (VMs) as well as to devices that use personal vDisks.

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

The wizard:

- creates VMs on a XenDesktop-hosted hypervisor using an existing machine template:
  - XenServer
  - ESX via V-Center
  - Hyper-V using SCVMM (when provisioning to a 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 Provisioning Services target devices within a new or existing Provisioning Services Device Collection matching the XenDesktop 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 XenDesktop catalog.

> **Note**
>
> For XenDesktop SetUp Wizard provisioned Gen 2 VMs, the BDM partition is FAT formatted with a drive letter. As a result, Windows in a PVS private image should be aware of the new partition. For example, a RDS PVS image using a writecache disk and BDM partition should see 2 partitions in private image mode.

When using the Linux streaming feature, consider that a new step was added to the XenDesktop Setup Wizard. You must add the SOAP SSL certificate to ensure that the Linux target can image the vDisk through the SOAP server. Refer to theinstallation article for more information.

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 Provisioning Services 7.x.

Write cache considerations

To minimize the time it takes to provision, the XenDesktop Set Up Wizard discards any hard disks that are attached to a template.

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, Provisioning Services 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 ESX and Hyper-V, you cannot use the Citrix Virtual Apps and Desktops Setup Wizard to provision VMs if you are using hypervisor local storage.

> **Important**
>
> When specifying names associated with storage devices, do not use a comma (,). Names associated with storage devices are retained by XenDesktop and separated by commas. For example, Storage 1, Storage 2, Storage 3. If a storage name includes a comma (for instance, 'Storage1,East') PVS erroneously recognizes this as two separate storage devices.

Virtual disk types

VMs provisioned through the XenDesktop Setup Wizard have new disks created and attached for local Provisioning Services 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 reg key to override the default types of write cache disks created by provisioning deployments on SCVMM and ESX. This 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"will override to dynamic. Remove the key to return to default behavior.

Run the wizard

Run the wizard directly from the Provisioning Services Console or from a remote console.

1. Right-click on any Site icon in the Console tree panel, then select the XenDesktop Setup Wizard …menu option. The XenDesktop Setup Wizard appears.
2. Click Next to begin setup.
3. On the XenDesktop Host page, enter the location of the XenDesktop Host address to connect to and to configure. The most recently used XenDesktop 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 setting are added in XenDesktop 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 XenDesktop 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 new 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 new 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.
     - Note that vGPU 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 additional 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 in option a 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, not 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 new accounts
    - Import existing accounts

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

12. To Create new accounts: An Active Directory administrator needs to delegate rights to the Provisioning Services 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 those 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 will dynamically replace 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 already exist in any of the following locations, they are not valid and do not display in the list; XenDesktop (as a machine), PVS (as a device), on the hypervisor (as a VM). If the AD structure contains a large number of objects or containers, or you are importing a large amount of machine accounts, the import may take a while as it must validate that each imported account does not already exist in Provisioning Services, XenDesktop, and the destination hypervisor. If this is the case, 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 Provisioning Services 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.
- Provisioning Services 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 Provisioning Services software and drivers, then reassigning 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 Provisioning Services with Nutanix Acropolis:

- An installed Nutanix Acropolis hypervisor plugin for PVS.
- 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:

- 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 will be 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* prior to imaging.

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

SCVMM requirements

Consider the following:

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

Provisioning vGPU-enabled XenDesktop machines

January 12, 2023

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 PVS. PVS only uses the vGPU setting in the template and propagates it to the VMs

> provisioned by the XenDesktop Setup Wizard.

- A server capable of hosting XenServer and NVIDIA GRID cards. For details on recommended hardware, refer to the XenServer system requirements.
- 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 (available from http://www.nvidia.com/vGPU).
- The Provisioning Services release that corresponds to the XenDesktop release you are using. The Provisioning Services XenDesktop Setup Wizard only works with the corresponding XenDesktop controller.
- To provision machines using the Provisioning Services XenDesktop Setup Wizard, you must use Provisioning Services 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 Provisioning Services Streamed Virtual Machine Setup Wizard.
- For details on configuring vGPU for XenServer, see Prepare host for graphics.

> **Note**
>
> XenDesktop 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 Provisioning Services Target Device software.
5. Using the Provisioning Services Imaging Wizard, create a master vDisk image. If you plan to use the XenDesktop Setup Wizard to provision machines, you must select the **Target Device Optimizer** when creating the vDisk image, otherwise the VM may fail 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 XenDesktop Virtual Delivery Agent

1. Using the Provisioning Services Console, set the vDisk image mode to Private Image.
2. Install the XenDesktop Virtual Delivery Agent (VDA) and point the VDA to the XenDesktop Server during the installation. .
   Note: Alternatively, you can chose to install both the VDA and the target device software prior to 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 XenDesktop VMs

1. Using the Provisioning Services 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 Provisioning Services XenDesktop Setup Wizard to provision VMs. This method is available only if you are using Provisioning Services 7.7 or later and XenDesktop 7.7 or later.
   - Run the Provisioning Services 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 XenDesktop 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 XenDesktop management while physical machine catalogs do not.

Virtual and blade server machine catalogs Requirements:

- For XenDesktop, 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 Provisioning Services device collection, and the Active Directory record must all be the same.

Steps:

1. Start the XenDesktop Machine Catalog Setup Wizard, then select **Windows Desktop OS** on the Operating System page.
2. On the Machine Management page, for *This Machine Catalog uses* select **Machines that are power managed**.
3. For *Deploy machines using:* select **Citrix Provisioning Services (PVS)**. Power management is provided by XenDesktop.
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 Provisioning Services structure that displays, select the Provisioning Services 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 Requirements:

Device names must exist in the Provisioning Services device collection and in Active Directory. **Note:** The XenDesktop host record is not required and the VM record names are not checked.

Steps:

1. Start the XenDesktop Machine Catalog Setup Wizard, then select **Windows Desktop OS** on the Operating System page.
2. On the Machine Management page, for *This Machine Catalog uses* select **Machines that are power managed**.
3. For *Deploy machines using:* select **Citrix Provisioning Services (PVS)**. Power management will be provided by XenDesktop.
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 Provisioning Services structure that displays, select the Provisioning Services 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**.

Create a Delivery Group and associate it with the machine catalog

For details on creating a Delivery Group, refer to the XenDesktop documentation.

PVS and XenDesktop cloud considerations

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

Configuring Personal vDisks

December 28, 2018

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

Provisioning Services target devices that use personal vDisks are created using the Citrix XenDesktop Setup Wizard. Within a Provisioning Services farm, the wizard creates target devices and adds target devices to an existing site's collection. The wizard then assigns an existing vDisk, which is in standard image mode, to that device.

The wizard also creates XenDesktop virtual machines to associate with each Provisioning Services target device. A catalog exists in Citrix Desktop Studio that allows you to preserve the assignment of users to desktops. The same users are assigned the same desktop for later sessions. In addition, a dedicated storage disk is created (before logon) for each user so they can store all personalization's to that desktop (personal vDisk). Personalizations include any changes to the vDisk image or desktop that are not made as a result of an image update. Examples include application settings, adds, deletes, modifications, or documents. Target devices using personal vDisks can also be reassigned a different vDisk if that vDisk is from the same base vDisk lineage. For additional information on using personal vDisks with XenDesktop, refer to XenDesktop's About Personal vDisks topic.

Inventory is run when a Provisioning Services vDisk is configured or updated. The method selected to configure or update a vDisk image for use as a personal vDisk image determines when vDisk inventory runs in your deployment. The following sections identify the different methods from which you can choose. It provides the high-level tasks associated with each method, and indicates at which point inventory runs for each method.

After configuring and adding a new personal vDisk image, do not use your golden VM as the machine template. It creates an unnecessary large disk as your write cache disk (the size of your original HDD).

Configure and deploy a new personal vDisk image

Configuration methods include:

- Configure in the following order: Provisioning Services, then capture the image, then XenDesktop
- Configure in the following order: Provisioning Services, then XenDesktop, then capture the image
- Configure in the following order: XenDesktop, then Provisioning Services, then capture the image
- Configure using Machine Creation Services (MCS)

Provisioning Services, then capture image, then XenDesktop

1. Install and configure the OS on a VM.
2. Install the Provisioning Services target device software on the VM.
3. Run the Provisioning Services Imaging Wizard to configure the vDisk.
4. Reboot.
5. The Provisioning Services Image Wizard's second stage runs to capture the personal vDisk image.
6. From the Console, set the target device to boot from the vDisk.
7. Configure the VM to boot from the network, then reboot.
8. Install XenDesktop software on the VM, then configure with advanced options for personal vDisk.
9. Manually run inventory, then shut the VM down.
10. From the Console, place the vDisk in Standard Image Mode. Image is ready for deployment.

Provisioning Services, then XenDesktop, then capture image

1. Install and configure the OS in a VM.
2. Install the Provisioning Services target device software on the VM.
3. Install XenDesktop software and configure with advanced options for personal vDisks enabled.
4. Reboot.
5. Log on to the VM.
6. Run the Provisioning Services Imaging Wizard on the VM to configure the vDisk. (Inventory automatically runs after the VM successfully shuts down and reboots.)
7. The Imaging Wizard's second stage runs to capture the personal vDisk image.
8. Shut the VM down.
9. From the Console, place the personal vDisk image in Standard Image Mode. The personal vDisk is ready for deployment.
10. Before using a VM template to provision multiple VMs to a XenDesktop site, verify the new vDisk can successfully boot from the VM created to serve as the machine template (not the golden VM).

Verify the write cache disk is recognized successfully:

a) Place the vDisk image in Private Image mode.
b) Boot the new vDisk image from the VM.
c) Format the new write cache partition manually.
d) Shut down the VM. During the shutdown process, when prompted run personal vDisk inventory.
e) Turn this VM into a template.

XenDesktop, then Provisioning Services, then capture image

1. Install and configure the OS in a VM.
2. Install XenDesktop software on the VM, then configure with advanced options for personal vDisk enabled.
3. Reboot.
4. Log on to, then shutdown the VM. Inventory automatically runs at shutdown.
5. Log on to, then install the Provisioning Service's target device software.
6. Run the Provisioning Services Imaging Wizard on the VM to configure the vDisk.
7. Reboot. (Inventory automatically runs after the VM successfully shuts down and reboots.)
8. The Imaging Wizard's second stage runs to capture the personal vDisk image.
9. Shut the VM down.
10. Place the vDisk in Standard Image Mode. The personal vDisk is ready for deployment.
11. Before using a VM template to provisioning multiple VMs to a XenDesktop site, verify the new vDisk can successfully boot from the VM created to serve as the machine template (not the golden VM), and verify the write cache disk is recognized successfully:

    a) Place the vDisk image in Private Image mode.
    b) Boot the new vDisk image from the VM.
    c) Format the new write cache partition manually.
    d) Shut down the VM. During the shutdown process, when prompted run personal vDisk inventory.
    e) Turn this VM into a template.

MCS

1. Install and configure the OS in an MCS VM.
2. Install XenDesktop software and configure with advanced options for personal vDisks.
3. Reboot the VM.
4. Log on to the VM, and then shut the VM down. Inventory automatically runs at shutdown.
5. The personal vDisk image is ready for deployment.

Update an existing personal vDisk image

Updating existing personal vDisk methods include using:

- Provisioning Services</span>
- MCS</span>

Updates for both Provisioning Services and MCS must be done on VMs that do not have a personal vDisk.

Provisioning Services

1. Create a version of the vDisk image.
2. Boot the VM from the vDisk image in Maintenance Mode.
3. Install updates on the new vDisk version.
4. Shut the VM down. Inventory runs automatically when the VM shuts down.
5. Promote the new version to either Test or Production. Other VMs will have access to the updated vDisk version the next time they reboot.

MCS

1. Boot the 'golden'VM.
2. Install updates on the VM.
3. Shut the VM down. Inventory automatically runs when the VM is shut down.

For additional information on how to create a Provisioning Services target device that uses a personal vDisk, refer to Deploy virtual desktops to VMs using the XenDesktop Setup Wizard. To view the properties of a Provisioning Services target device configured to use a personal vDisk, refer to Configure target devices that use personal vDisks.

APIs

March 4, 2021

There are four APIs available with Provisioning Services. Each API has its own Programmer's Guide, listed below. 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

CIS Problem Reporting

June 17, 2021

Citrix Provisioning allows you to report problems you encounter while using the software directly to Citrix Support. The support team 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 Citrix Provisioning server, or for a site:

- If you have an environment with multiple provisioning servers, each has had a different SOAP Service user. In such environments, the SOAP Service user must have read\write permissions to the network share when generating the diagnostic bundle.

- If you are reporting a problem for a specific provisioning server, only that server generates a diagnostic bundle that captures the event.
- If you are reporting a problem for a site, each provisioning server in the site generates a diagnostic bundle.
- Upload the diagnostic bundle directly to Citrix, or save it to a shared network drive and manually upload it later.

> **Note:**
>
> The diagnostic bundle is manually uploaded to the Citrix CIS website. Log in to this site using your Citrix credentials.

Report a problem using the NETWORK SERVICE user account

You can set up your system to generate problem reports for the NETWORK SERVICE user.

To enable the NETWORK SERVICE user to collect information and read from the registry, first make NETWORK SERVICE a local admin of your Provisioning server. Then give the user read/write permissions to the network share where the report is generated.

To make the NETWORK SERVICE user a local admin of your Provisioning server:

1. Log in to the VM as a local administrator.
2. From the Start menu, select **Administrative tools > Computer Management > Groups > Users**.
3. Add the user NETWORK SERVICE. From the Select Users dialog box, select **Location** and verify that you're adding the user to the local VM.
4. Add the user NETWORK SERVICE to the Administrators group. From the Start menu, select **Administrative tools > Computer Management > Groups > Administrators**. From the Select Users dialog box, select **Location** and verify that you're adding the administrator to the local VM.

To give the NETWORK SERVICE user read/write permissions to the network share:

1. Right-click the network shared folder and select **Folder > Properties**. On the Sharing tab, set the folder to **Shared**.
2. On the Security tab, make sure the NETWORK SERVICE user has read/write permissions.
3. In the Citrix Provisioning Configuration Wizard, select **Network service account** as the Stream and SOAP Services user account. This gives the NETWORK SERVICE user read/write access to `ProgramData\Citrix\Provisioning Services`, where the report files are generated until upload.

Using a token for the secure communication

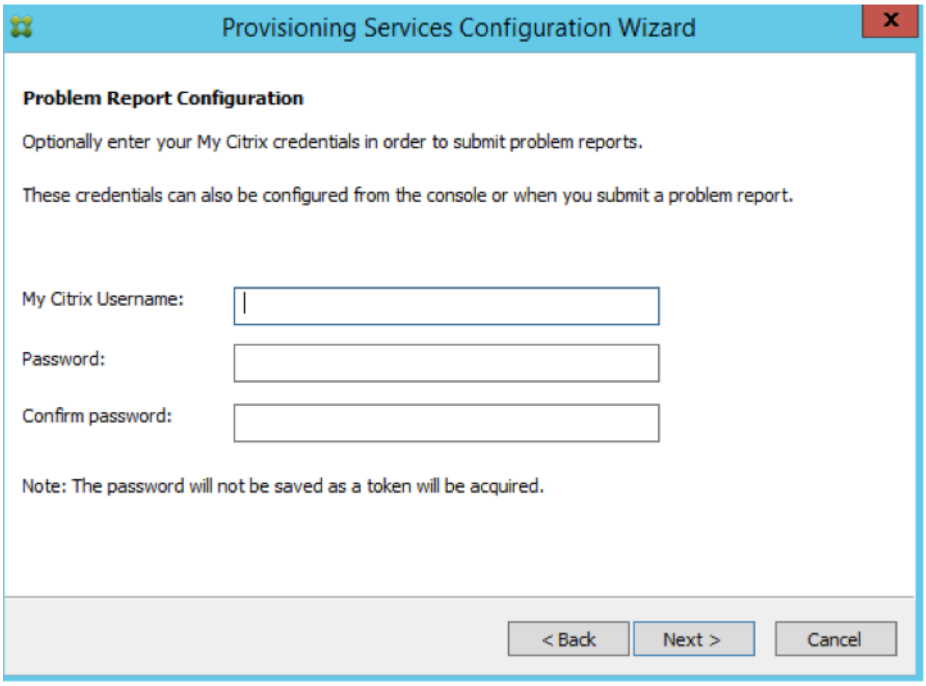
When using problem reporting, a token is generated to associate the diagnostic bundle with your My Citrix account login credentials. Once the token is associated with your My Citrix credentials, it's stored in the database for future problem reporting. This process eliminates the need to store your login credentials.

> **Note:**
>
> If you are using Problem Reporting for the first time and have not yet configured a login token, you are prompted to enter your My Citrix login credentials. Once you enter your login credentials, the token is generated in the database.

Configure the problem reporting feature

In the **Citrix Provisioning Configuration Wizard** screen:

1. Enter your Citrix user name and password.
2. Confirm the password.
3. Click **Next**.



Problem Report Configuration

Optionally enter your My Citrix credentials in order to submit problem reports.

These credentials can also be configured from the console or when you submit a problem report.

My Citrix Username:

Password:

Confirm password:

Note: The password will not be saved as a token will be acquired.

> **Tip:**
>
> If you don't have a secure token to authenticate your login credentials, the **Problem Report Configuration** screen indicates that *The token required to submit problem reports is empty. Please reconfigure.* The token can be generated by entering your credentials here or later using the Citrix

> Provisioning console.

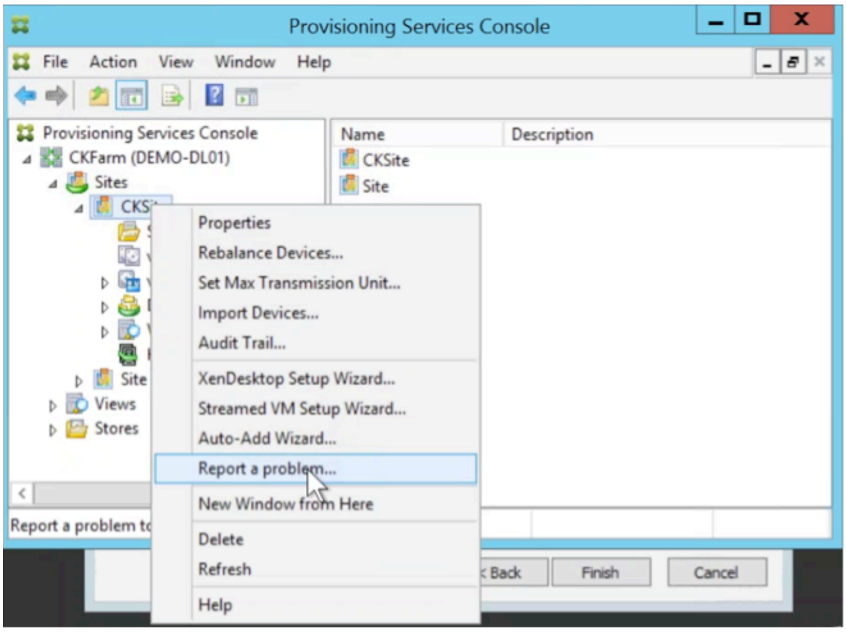
The password and user name you specify are not saved. The token that is generated is used to associate your diagnostics bundle with your My Citrix account.

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 user name, or you can generate diagnostic information locally to a ZIP file. Select an empty folder on a shared network drive accessible to all servers included in this problem report.

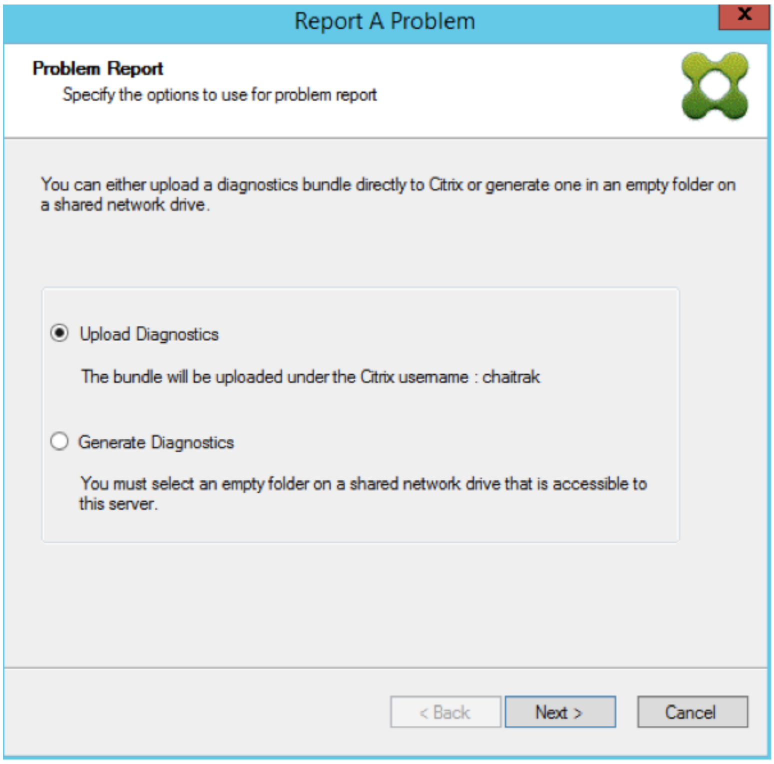
To report a problem

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 the 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**.



Problem Report

Specify the options to use for problem report

You can either upload a diagnostics bundle directly to Citrix or generate one in an empty folder on a shared network drive.

● Upload Diagnostics

The bundle will be uploaded under the Citrix username : chaitrak

○ Generate Diagnostics

You must select an empty folder on a shared network drive that is accessible to this server.

> **Note:**
>
> Each server in the selected site uploads or generates its own diagnostic bundle.
>
> The token is only required for an 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.

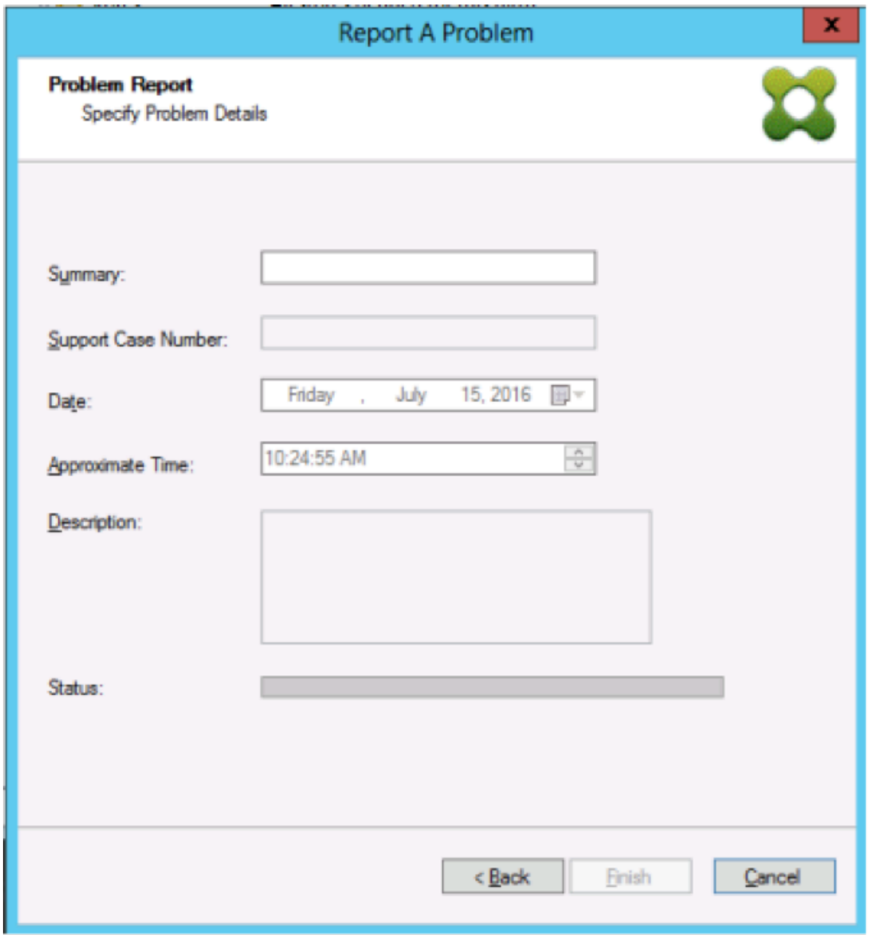
   b. Optionally enter a support case number.

   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**.



Report A Problem

Problem Report

Specify Problem Details

Summary:

Support Case Number:

Date: Friday , July 15, 2016

Approximate Time: 10:24:55 AM

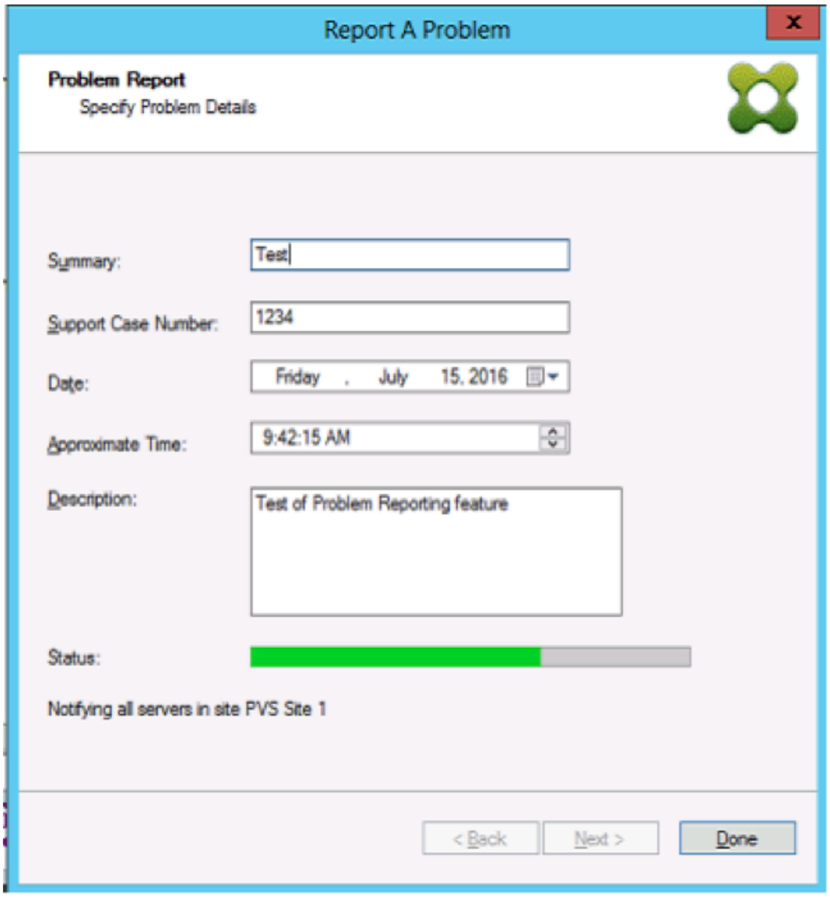
Description:

Status:

> **Tip:**
>
> After finishing the diagnostic report, the bundle is created on the server 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.

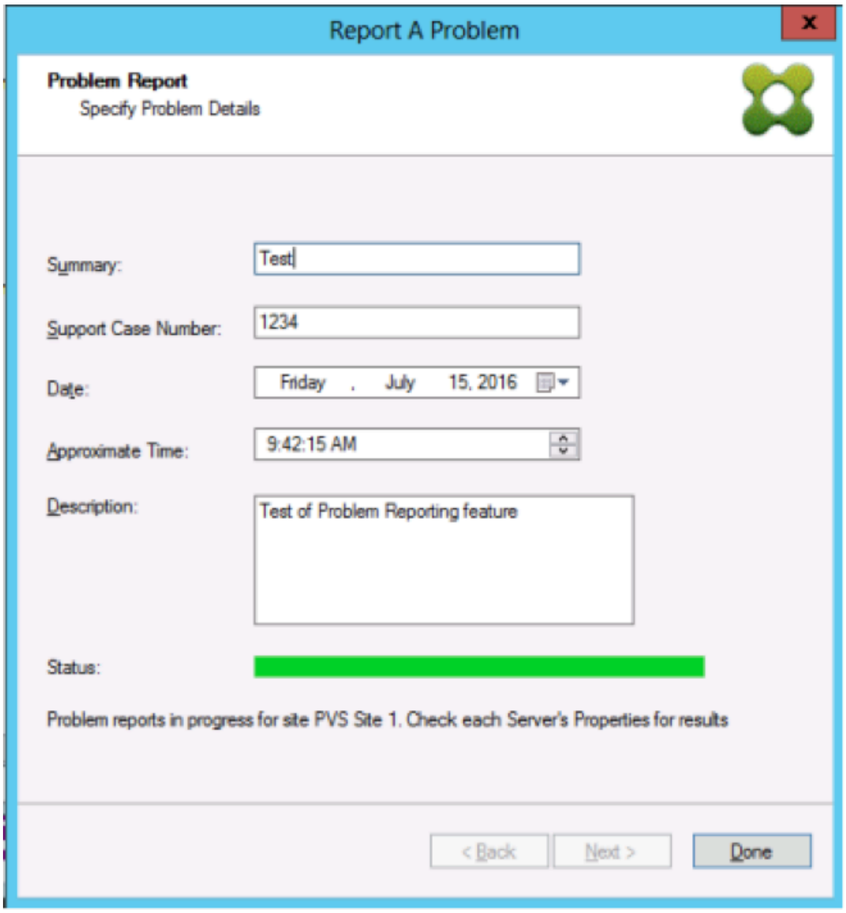
The **Status** field displays information about the state of the reporting mechanism. Once the process starts, use the **Done** button to dismiss the dialog to allow the process to continue in the background:



Problem Report
Specify Problem Details

Summary: Test
Support Case Number: 1234
Date: Friday , July 15, 2016
Approximate Time: 9:42:15 AM
Description: Test of Problem Reporting feature
Status:
Notifying all servers in site PVS Site 1

If you choose not to dismiss the dialog, the process continues in the foreground. Once completed, the **Problem Report** screen provides additional information *Check each Server's Properties for results.* With this message, each server has completed the problem report generation process and saves the results.



Summary: Test

Support Case Number: 1234

Date: Friday , July 15, 2016

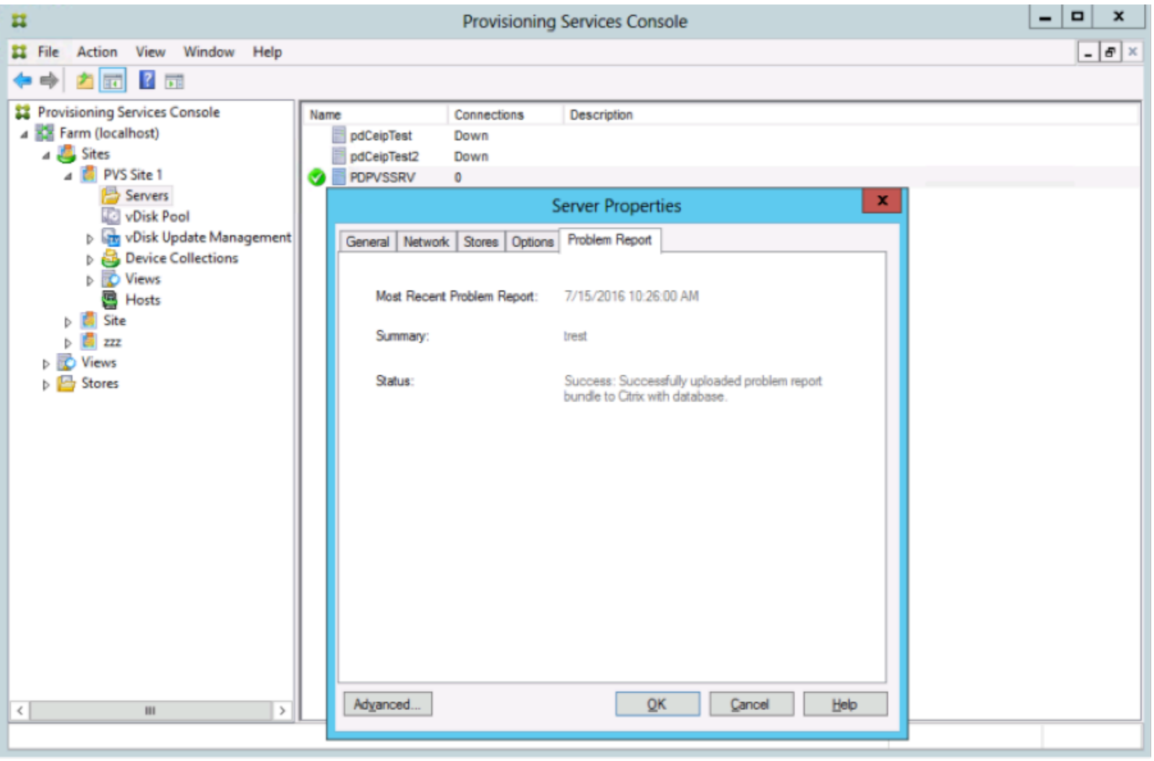
Approximate Time: 9:42:15 AM

Description: Test of Problem Reporting feature

Status:

Problem reports in progress for site PVS Site 1. Check each Server's Properties for results

Once the problem report is generated, you can view the results in the **Properties** screen. To view the report, select **Server>Properties**.



Most Recent Problem Report: 7/15/2016 10:26:00 AM

Summary: trest

Status: Success: Successfully uploaded problem report bundle to Citrix with database.

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. The information is generated from the mandatory summary field specified when the administrator first created the report.
- **Status**. Describes the status of the most recent report. It indicates:
  - Success or failure
  - Whether the report was 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.