Setting Up Virtual Desktops in Horizon 7

VMware Horizon 7 7.1

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Setting Up Virtual Desktops in Horizon 7

1

Setting Up Virtual Desktops in Horizon 7 describes how to create and provision pools of virtual machines. It includes information about preparing machines, provisioning desktop pools, and configuring user profiles with View Persona Management.

Intended Audience

This information is intended for anyone who wants to create and provision desktop and application pools. The information is written for experienced Windows system administrators who are familiar with virtual machine technology and datacenter operations.

Introduction to Virtual Desktops 2

With Horizon 7, you can create desktop pools that include thousands of virtual desktops. You can deploy desktops that run on virtual machines (VMs) and physical machines. Create one VM as a base image, and Horizon 7 can generate a pool of virtual desktops from that image.

This chapter includes the following topics:

- "Virtual Desktop Pools," on page 9
- "Advantages of Desktop Pools," on page 9
- "Desktop Pools for Specific Types of Workers," on page 10

Virtual Desktop Pools

You can create desktop pools to give users remote access to virtual machine-based desktops. You can also choose VMware PC-over-IP (PCoIP), or VMware Blast to provide remote access to users.

There are two main types of virtual desktop pools: automated and manual. Automated desktop pools use a vCenter Server virtual machine template or snapshot to create a pool of identical virtual machines. Manual desktop pools are a collection of existing vCenter Server virtual machines, physical computers, or third-party virtual machines. In automated or manual pools, each machine is available for one user to access remotely at a time.

Advantages of Desktop Pools

Horizon 7 offers the ability to create and provision pools of desktops as its basis of centralized management.

You create a remote desktop pool from one of the following sources:

- A physical system such as a physical desktop PC.
- A virtual machine that is hosted on an ESXi host and managed by vCenter Server
- A virtual machine that runs on a virtualization platform other than vCenter Server that supports Horizon Agent.

If you use a vSphere virtual machine as a desktop source, you can automate the process of making as many identical virtual desktops as you need. You can set a minimum and maximum number of virtual desktops to be generated for the pool. Setting these parameters ensures that you always have enough remote desktops available for immediate use but not so many that you overuse available resources.

Using pools to manage desktops allows you to apply settings or deploy applications to all remote desktops in a pool. The following examples show some of the settings available:

- Specify which remote display protocol to use as the default for the remote desktop and whether to let end users override the default.

- For View Composer linked-clone virtual machines or full clone virtual machines, specify whether to power off the virtual machine when it is not in use and whether to delete it altogether. Instant clone virtual machines are always powered on.
- For View Composer linked-clone virtual machines, you can specify whether to use a Microsoft Sysprep customization specification or QuickPrep from VMware. Sysprep generates a unique SID and GUID for each virtual machine in the pool. Instant clones require a different customization specification, called ClonePrep, from VMware.

You can also specify how users are assigned desktops in a pool.

Dedicated-assignment pools

Each user is assigned a particular remote desktop and returns to the same desktop at each login. Dedicated assignment pools require a one-to-one desktop-to-user relationship. For example, a pool of 100 desktops are needed for a group of 100 users.

Floating-assignment pools

The remote desktop is optionally deleted and re-created after each use, offering a highly controlled environment.

Using floating-assignment pools also allows you to create a pool of desktops that can be used by shifts of users. For example, a pool of 100 desktops could be used by 300 users if they worked in shifts of 100 users at a time.

Desktop Pools for Specific Types of Workers

View provides many features to help you conserve storage and reduce the amount of processing power required for various use cases. Many of these features are available as pool settings.

The most fundamental question to consider is whether a certain type of user needs a stateful desktop image or a stateless desktop image. Users who need a stateful desktop image have data in the operating system image itself that must be preserved, maintained, and backed up. For example, these users install some of their own applications or have data that cannot be saved outside of the virtual machine itself, such as on a file server or in an application database.

Stateless desktop images

Also known as nonpersistent desktops, stateless architectures have many advantages, such as being easier to support and having lower storage costs. Other benefits include a limited need to back up the virtual machines and easier, less expensive disaster recovery and business continuity options.

Stateful desktop images

Also known as persistent desktops, these images might require traditional image management techniques. Stateful images can have low storage costs in conjunction with certain storage system technologies. Backup and recovery technologies such as VMware Consolidated Backup and VMware Site Recovery Manager are important when considering strategies for backup, disaster recovery, and business continuity.

There are two ways to create stateless desktop images in View:

- You can create floating assignment pools of instant clone virtual machines. Folder redirection and roaming profiles can optionally be used to store user data.
- You can use View Composer to create floating assignment pools of linked clone virtual machines. Folder redirection and roaming profiles can optionally be used to store user data.

There are several ways to create stateful desktop images in View:

- You can create floating assignment pools of instant clone virtual machines and use App Volumes to attach user data and user-installed apps. Folder redirection and roaming profile can optionally be used to store user data.

- You can use View Composer to create dedicated assignment pools of linked clone virtual machines. You can configure View Composer persistent disks.
- You can create full clones or full virtual machines. Some storage vendors have cost-effective storage solutions for full clones. These vendors often have their own best practices and provisioning utilities. Using one of these vendors might require that you create a manual dedicated-assignment pool.

Whether you use stateless or stateful desktops depends on the specific type of worker.

Pools for Task Workers

You can standardize on stateless desktop images for task workers so that the image is always in a well-known, easily supportable configuration and so that workers can log in to any available desktop.

Because task workers perform repetitive tasks within a small set of applications, you can create stateless desktop images, which help conserve storage space and processing requirements. Use the following pool settings:

- Create an automated pool so that desktops can be created when the pool is created or can be generated on demand based on pool usage.
- For instant clone pools, to optimize resource utilization, use on demand provisioning to grow or shrink the pool based on usage. Be sure to specify enough spare desktops to satisfy the login rate.
- Use floating assignment so that users log in to any available desktop. This setting reduces the number of desktops required if everyone does not need to be logged in at the same time.
- Create instant-clone or View Composer linked-clone desktops so that desktops share the same base image and use less storage space in the datacenter than full virtual machines.
- For View Composer desktop pools, determine what action, if any, to take when users log off. Disks grow over time. You can conserve disk space by refreshing the desktop to its original state when users log off. You can also set a schedule for periodically refreshing desktops. For example, you can schedule desktops to refresh daily, weekly, or monthly.
- For instant clone desktop pools, View automatically deletes the instant clone whenever a user logs out. A new instant clone is created and ready for the next user to log in, thus effectively refreshing the desktop on every log out.
- If applicable, and if you use View Composer linked-clone pools, consider storing desktops on local ESXi data stores. This strategy can offer advantages such as inexpensive hardware, fast virtual-machine provisioning, high-performance power operations, and simple management. For a list of the limitations, see "Storing View Composer Linked Clones on Local Datastores," on page 154. Instant clone pools are not supported on local data stores.

  Note For information about other types of storage options, see Chapter 11, "Reducing and Managing Storage Requirements," on page 139.

- Use the Persona Management feature so that users always have their preferred desktop appearance and application settings, as with Windows user profiles. If you do not have the desktops set to be refreshed or deleted at logoff, you can configure the persona to be removed at logoff.

Important View Persona Management facilitates implementing a floating-assignment pool for those users who want to retain settings between sessions. Previously, one of the limitations of floating-assignment desktops was that when end users logged off, they lost all their configuration settings and any data stored in the remote desktop.

Each time end users logged on, their desktop background was set to the default wallpaper, and they would have to configure each application's preferences again. With View Persona Management, an end user of a floating-assignment desktop cannot tell the difference between their session and a session on a dedicated-assignment desktop.

Pools for Knowledge Workers and Power Users

Knowledge workers must be able to create complex documents and have them persist on the desktop. Power users must be able to install their own applications and have them persist. Depending on the nature and amount of personal data that must be retained, the desktop can be stateful or stateless.

For knowledge workers who do not need user-installed applications except for temporary use, you can create stateless desktop images and save all their personal data outside of the virtual machine, on a file server or in an application database. For other knowledge workers and for power users, you can create stateful desktop images. Use the following pool settings:

- Some power users and knowledge workers, such as accountants, sales managers, marketing research analysts, might need to log into the same desktop every time. Create dedicated assignment pools for them.
- Use the Persona Management feature so that users always have their preferred desktop appearance and application settings, as with Windows user profiles.
- Use vStorage thin provisioning so that at first, each desktop uses only as much storage space as the disk needs for its initial operation.
- For power users and knowledge workers who must install their own applications, which adds data to the operating system disk, there are two options. One option is to create full virtual machine desktops, and use Mirage to deploy and update applications without overwriting user-installed applications.

  The other option is to create a pool of linked clones or instant clones, and use App Volumes to persist user-installed applications and user data across logins.
- If knowledge workers do not require user-installed applications except for temporary use, you can create View Composer linked-clone desktops or instant clone desktops. The desktop images share the same base image and use less storage space than full virtual machines.
- If you use View Composer with vSphere 5.1 or later virtual desktops, enable the space reclamation feature for vCenter Server and for the desktop pool. With the space reclamation feature, stale or deleted data within a guest operating system is automatically reclaimed with a wipe and shrink process.
- If you use View Composer linked-clone desktops, implement View Persona Management, roaming profiles, or another profile management solution. You can also configure persistent disks so that you can refresh and recompose the linked-clone OS disks while keeping a copy of the user profile on the persistent disks.
- If you use instant clone desktops, implement roaming profiles or another profile management solution. You do not need to configure persistent disks. You can use App Volumes to retain a copy of the user data and profile.

Pools for Kiosk Users

Kiosk users might include customers at airline check-in stations, students in classrooms or libraries, medical personnel at medical data entry workstations, or customers at self-service points. Accounts associated with client devices rather than users are entitled to use these desktop pools because users do not need to log in to use the client device or the remote desktop. Users can still be required to provide authentication credentials for some applications.

Virtual machine desktops that are set to run in kiosk mode use stateless desktop images because user data does not need to be preserved in the operating system disk. Kiosk mode desktops are used with thin client devices or locked-down PCs. You must ensure that the desktop application implements authentication mechanisms for secure transactions, that the physical network is secure against tampering and snooping, and that all devices connected to the network are trusted.

As a best practice, use dedicated View Connection Server instances to handle clients in kiosk mode, and create dedicated organizational units and groups in Active Directory for the accounts of these clients. This practice not only partitions these systems against unwarranted intrusion, but also makes it easier to configure and administer the clients.

To set up kiosk mode, you must use the `vdmadmin` command-line interface and perform several procedures documented in the topics about kiosk mode in the *View Administration* document. As part of this setup, you can use the following pool settings.

- Create an automated pool so that desktops can be created when the pool is created or can be generated on demand based on pool usage.
- Use floating assignment so that users can access any available desktop in the pool.
- Create instant-clone or View Composer linked-clone desktops so that desktops share the same base image and use less storage space in the datacenter than full virtual machines.
- If you are using View Composer linked-clone desktops, institute a refresh policy so that the desktop is refreshed frequently, such as at every user logoff.
- If you are using instant clone desktop pools, View automatically deletes the instant clone whenever a user logs out. A new instant clone is created and ready for the next user to log in, thus effectively refreshing the desktop on every log out.
- If applicable, consider storing desktops on local ESXi datastores. This strategy can offer advantages such as inexpensive hardware, fast virtual-machine provisioning, high-performance power operations, and simple management. For a list of the limitations, see "Storing View Composer Linked Clones on Local Datastores," on page 154. Instant clone pools are not supported on local data stores.

  NOTE For information about other types of storage options, see Chapter 11, "Reducing and Managing Storage Requirements," on page 139.

- Use an Active Directory GPO (group policy object) to configure location-based printing, so that the desktop uses the nearest printer. For a complete list and description of the settings available through Group Policy administrative (ADM) templates, see *Configuring Remote Desktop Features in Horizon 7*.
- Use a GPO or Smart Policies to control whether local USB devices are connected to the desktop when the desktop is launched or when USB devices are plugged in to the client computer.

Preparing Unmanaged Machines 3

Users can access remote desktops delivered by machines that are not managed by vCenter Server. These unmanaged machines can include physical computers and virtual machines running on virtualization platforms other than vCenter Server. You must prepare an unmanaged machine to deliver remote desktop access.

For information about preparing machines that are used as Remote Desktop Services (RDS) hosts, see *Setting Up RDS Desktops and Applications in Horizon 7* guide.

For information about preparing Linux virtual machines for remote desktop deployment, see the *Setting Up Horizon 7 for Linux Desktops* guide.

This chapter includes the following topics:

- "Prepare an Unmanaged Machine for Remote Desktop Deployment," on page 15
- "Install Horizon Agent on an Unmanaged Machine," on page 16

Prepare an Unmanaged Machine for Remote Desktop Deployment

You must perform certain tasks to prepare an unmanaged machine for remote desktop deployment.

Prerequisites

- Verify that you have administrative rights on the unmanaged machine.
- To make sure that remote desktop users are added to the local Remote Desktop Users group of the unmanaged machine, create a restricted Remote Desktop Users group in Active Directory. See the *View Installation* document for more information.

Procedure

1 Power on the unmanaged machine and verify that it is accessible to the View Connection Server instance.

2 Join the unmanaged machine to the Active Directory domain for your remote desktops.

3 Configure the Windows firewall to allow Remote Desktop connections to the unmanaged machine.

What to do next

Install Horizon Agent on the unmanaged machine. See "Install Horizon Agent on an Unmanaged Machine," on page 16.

Install Horizon Agent on an Unmanaged Machine

You must install Horizon Agent on an all unmanaged machines. View cannot manage an unmanaged machine unless Horizon Agent is installed.

To install Horizon Agent on multiple Windows physical computers without having to respond to wizard prompts, you can install Horizon Agent silently. See "Install Horizon Agent Silently," on page 30.

Prerequisites

- Verify that you have administrative rights on the unmanaged machine.
- To use an unmanaged Windows Server machine as a remote desktop rather than as an RDS host, perform the steps described in "Prepare Windows Server Operating Systems for Desktop Use," on page 24.
- Familiarize yourself with the Horizon Agent custom setup options for unmanaged machines. See "Horizon Agent Custom Setup Options for Unmanaged Machines," on page 17.
- Familiarize yourself with the TCP ports that the Horizon Agent installation program opens on the firewall. See the *View Architecture Planning* document for more information.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at http://www.vmware.com/go/downloadview.

Procedure

1. To start the Horizon Agent installation program, double-click the installer file.

   The installer filename is `VMware-viewagent-`*`y.y.y`*`-`*`xxxxxx`*`.exe` or `VMware-viewagent-x86_64-`*`y.y.y`*`-`*`xxxxxx`*`.exe`, where *y.y.y* is the version number and *xxxxxx* is the build number.

2. Accept the VMware license terms.
3. Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

   You must install all View components with the same IP version.

4. Select whether to enable or disable FIPS mode.

   This option is available only if FIPS mode is enabled in Windows.

5. Select your custom setup options.
6. Accept or change the destination folder.
7. In the **Server** text box, type the host name or IP address of a View Connection Server host.

   During installation, the installer registers the unmanaged machine with this View Connection Server instance. After registration, the specified View Connection Server instance, and any additional instances in the same View Connection Server group, can communicate with the unmanaged machine.

8 Select an authentication method to register the unmanaged machine with the View Connection Server instance.

Option	Action
Authenticate as the currently logged in user	The **Username** and **Password** text boxes are disabled and you are logged in to the View Connection Server instance with your current username and password.
Specify administrator credentials	You must provide the username and password of a View Connection Server administrator in the **Username** and **Password** text boxes.

Provide the username in the following format: **`Domain\User`**.

The user account must be a domain user with access to View LDAP on the View Connection Server instance. A local user does not work.

9 Follow the prompts in the Horizon Agent installation program and finish the installation.

10 If you selected the USB redirection option, restart the unmanaged machine to enable USB support.

In addition, the **Found New Hardware** wizard might start. Follow the prompts in the wizard to configure the hardware before you restart the unmanaged machine.

The VMware Horizon Horizon Agent service is started on the unmanaged machine.

What to do next

Use the unmanaged machine to create a remote desktop. See "Manual Desktop Pools," on page 93.

Horizon Agent Custom Setup Options for Unmanaged Machines

When you install Horizon Agent on an unmanaged machine, you can select or deselect certain custom setup options. In addition, Horizon Agent installs certain features automatically on all guest operating systems on which they are supported. These features are not optional.

To change custom setup options after you install the latest Horizon Agent version, you must uninstall and reinstall Horizon Agent. For patches and upgrades, you can run the new Horizon Agent installer and select a new set of options without uninstalling the previous version.

Table 3-1. Horizon Agent Custom Setup Options for Unmanaged Machines in an IPv4 Environment (Optional)

Option	Description
USB Redirection	Gives users access to locally connected USB devices on their desktops. USB redirection is supported on remote desktops that are deployed on single-user machines. In addition, redirection of USB flash drives and hard disks is supported on RDS desktops and applications. This setup option is not selected by default. You must select the option to install it. For guidance on using USB redirection securely, see the *View Security* guide. For example, you can use group policy settings to disable USB redirection for specific users.
Client Drive Redirection	Allows Horizon Client users to share local drives with their remote desktops. After this setup option is installed, no further configuration is required on the remote desktop. Client Drive Redirection is also supported on VDI desktops that run on managed, single-user virtual machines and on RDS desktops and applications.

Table 3-1. Horizon Agent Custom Setup Options for Unmanaged Machines in an IPv4 Environment (Optional) (Continued)

Option	Description
View Persona Management	Synchronizes the user profile on the local desktop with a remote profile repository, so that users have access to their profiles whenever they log in to a desktop.
Smartcard Redirection	Lets users authenticate with smart cards when they use the PCoIP or Blast Extreme display protocol. Smartcard Redirection is supported on remote desktops that are deployed on single-user machines but is not supported on RDS host-based remote desktops.
Virtual audio driver	Provides a virtual audio driver on the remote desktop.

In an IPv6 environment, the only optional feature is Smartcard Redirection.

Table 3-2. Horizon Agent Features That Are Installed Automatically on Unmanaged Machines in an IPv4 Environment (Not Optional)

Feature	Description
PCoIP Agent	Lets users connect to the remote desktop with the PCoIP display protocol. The PCoIP Agent feature is supported on physical machines that are configured with a Teradici TERA host card.
Lync	Provides support for Microsoft Lync 2013 Client on remote desktops.
Unity Touch	Allows tablet and smart phone users to interact easily with Windows applications that run on the remote desktop. Users can browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications, all without using the Start menu or Taskbar.

In an IPv6 environment, the only automatically installed feature is PCoIP Agent.

Creating and Preparing a Parent Virtual Machine for Cloning 4

You can create a pool of desktop machines by cloning a vCenter Server virtual machine (VM). Before you create the desktop pool, you need to prepare and configure this VM, which will be the parent of the clones.

For information about preparing machines that are used as Remote Desktop Services (RDS) hosts, see the *Setting Up Desktops and Application Pools in Horizon 7* guide.

For information about preparing Linux VMs for remote desktop deployment, see the *Setting Up Horizon 7 for Linux Desktops* guide.

NOTE

- Starting with version 7.0, View Agent is renamed Horizon Agent and View Administrator is renamed Horizon Administrator.
- VMware Blast, the display protocol that is available starting with Horizon 7.0, is also known as VMware Blast Extreme.

This chapter includes the following topics:

Creating a Virtual Machine for Cloning

The first step in the process of deploying a pool of cloned desktops is to create a virtual machine in vSphere, install and configure the operating system.

1 Create a Virtual Machine in vSphere on page 20

  You can create a virtual machine in vSphere from scratch or by cloning an existing VM. This procedure describes creating a VM from scratch.

2 Install a Guest Operating System on page 22

After you create a virtual machine, you must install a guest operating system.

3 Prepare a Guest Operating System for Remote Desktop Deployment on page 22

You must perform certain tasks to prepare a guest operating system for remote desktop deployment.

4 Prepare Windows Server Operating Systems for Desktop Use on page 24

To use a Windows Server 2008 R2 or Windows Server 2012 R2 virtual machine as a single-session View desktop (rather than as an RDS host), you must perform certain steps before you install Horizon Agent in the virtual machine. You must also configure View Administrator to treat Windows Servers as supported operating systems for View desktop use.

5 Install Desktop Experience on Windows Server 2008 R2 on page 25

For RDS desktops and applications, and for VDI desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

6 Install Desktop Experience on Windows Server 2012 or 2012 R2 on page 26

For RDS desktops and applications, and for VDI desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

7 Configure the Windows Firewall Service to Restart After Failures on page 26

Some Windows Server 2012 R2, Windows 8.1, and Windows 10 machines that are deployed as single-session desktops do not become available immediately after they are provisioned. This issue occurs when the Windows Firewall service does not restart after its timeout period expires. You can configure the Windows Firewall service on the parent or template virtual machine to ensure that all machines in a desktop pool become available.

Create a Virtual Machine in vSphere

You can create a virtual machine in vSphere from scratch or by cloning an existing VM. This procedure describes creating a VM from scratch.

Prerequisites

- Familiarize yourself with the custom configuration parameters for virtual machines. See "Virtual Machine Custom Configuration Parameters," on page 21.

Procedure

1 Log in to vSphere Client.

2 Select **File > New > Virtual Machine** to start the New Virtual Machine wizard.

3 Select **Custom** and configure custom configuration parameters.

4 Select **Edit the virtual machine settings before completion** and click **Continue** to configure hardware settings.

   a Add a CD/DVD drive, set the media type to use an ISO image file, select the ISO image file of an appropriate operating system, and select **Connect at power on**.

   b Set **Power-on Boot Delay** to 10,000 milliseconds.

5 Click **Finish** to create the virtual machine.

What to do next

Install the operating system.

Virtual Machine Custom Configuration Parameters

You can use virtual machine custom configuration parameters as baseline settings when you create a virtual machine for remote desktop deployment.

You can change certain settings when you use View Administrator to deploy desktop pools from the virtual machine.

Table 4-1. Custom Configuration Parameters

Parameter	Description and Recommendations
`Name and Location`	The name and location of the virtual machine. If you plan to use the virtual machine as a template, assign a generic name. The location can be any folder within your datacenter inventory.
`Host/Cluster`	The ESXi server or cluster of server resources that will run the virtual machine. If you plan to use the virtual machine as a template, the location of the initial virtual machine does not necessarily specify where future virtual machines created from template will reside.
`Resource Pool`	If the physical ESXi server resources are divided into resource pools, you can assign them to the virtual machine.
`Datastore`	The location of files associated with the virtual machine.
`Hardware Machine Version`	The hardware machine version that is available depends on the ESXi version you are running. As a best practice, select the latest available hardware machine version, which provides the greatest virtual machine functionality. Certain View features require minimum hardware machine versions.
`Guest Operating System`	The type of operating system that you will install in the virtual machine.
`CPUs`	The number of virtual processors in the virtual machine. For most guest operating systems, a single processor is sufficient.
`Memory`	The amount of memory to allocate to the virtual machine. In most cases, 512MB is sufficient.
`Network`	The number of virtual network adapters (NICs) in the virtual machine. One NIC is usually sufficient. The network name should be consistent across virtual infrastructures. An incorrect network name in a template can cause failures during the instance customization phases. When you install Horizon Agent on a virtual machine that has more than one NIC, you must configure the subnet that Horizon Agent uses. See "Configure a Virtual Machine with Multiple NICs for Horizon Agent," on page 36 for more information. IMPORTANT For Windows 7, Windows 8.*, Windows 10, Windows Server 2008 R2, and Windows Server 2012 R2 operating systems, you must select the VMXNET 3 network adapter. Using the default E1000 adapter can cause customization timeout errors on virtual machines. To use the VMXNET 3 adapter, you must install a Microsoft hotfix: For Windows 7 SP1, install the following hotfixes: ■ http://support.microsoft.com/kb/2550978 Install the hotfix before installing Horizon Agent. When installing the hotfix, if you encounter Windows Update error 0x80070424, see https://support.microsoft.com/en-us/kb/968002. ■ https://support.microsoft.com/en-au/kb/2578159 ■ https://support.microsoft.com/en-au/kb/2661332 For more information on installing the hotfixes, see https://ikb.vmware.com/kb/2073945.

Table 4-1. Custom Configuration Parameters (Continued)

Parameter	Description and Recommendations
`SCSI Controller`	The type of SCSI adapter to use with the virtual machine. For Windows 8/8.1 and Windows 7 guest operating systems, you should specify the LSI Logic adapter. The LSI Logic adapter has improved performance and works better with generic SCSI devices. LSI Logic SAS is available only for virtual machines with hardware version 7 and later.
`Select a Disk`	The disk to use with the virtual machine. Create a new virtual disk based on the amount of local storage that you decide to allocate to each user. Allow enough storage space for the OS installation, patches, and locally installed applications. To reduce the need for disk space and management of local data, you should store the user's information, profile, and documents on network shares rather than on a local disk.

Install a Guest Operating System

After you create a virtual machine, you must install a guest operating system.

Prerequisites

- Verify that an ISO image file of the guest operating system is on a datastore on your ESXi server.
- Verify that the CD/DVD drive in the virtual machine points to the ISO image file of the guest operating system and that the CD/DVD drive is configured to connect at power on.

Procedure

1. In vSphere Client, log in to the vCenter Server system where the virtual machine resides.
2. Right-click the virtual machine, select **Power**, and select **Power On** to start the virtual machine.

   Because you configured the CD/DVD drive to point to the ISO image of the guest operating system and to connect at power on, the guest operating system installation process begins automatically.
3. Click the **Console** tab and follow the installation instructions provided by the operating system vendor.
4. Activate Windows.

What to do next

Prepare the guest operating system for View desktop deployment.

Prepare a Guest Operating System for Remote Desktop Deployment

You must perform certain tasks to prepare a guest operating system for remote desktop deployment.

Prerequisites

- Create a virtual machine and install a guest operating system.
- Configure an Active Directory domain controller for your remote desktops. See the *View Installation* document for more information.
- To make sure that desktop users are added to the local Remote Desktop Users group of the virtual machine, create a restricted Remote Desktop Users group in Active Directory. See the *View Installation* document for more information.

- Verify that Remote Desktop Services are started on the virtual machine. Remote Desktop Services are required for Horizon Agent installation, SSO, and other View operations. You can disable RDP access to your View desktops by configuring desktop pool settings and group policy settings. See "Prevent Access to Horizon 7 Desktops Through RDP," on page 128.
- Verify that you have administrative rights on the guest operating system.
- On Windows Server operating systems, prepare the operating system for desktop use. See "Prepare Windows Server Operating Systems for Desktop Use," on page 24.
- If you intend to configure 3D graphics rendering for desktop pools, familiarize yourself with the **Enable 3D Support** setting for virtual machines.

  This setting is active on Windows 7 and later operating systems. On ESXi 5.1 and later hosts, you can also select options that determine how the 3D renderer is managed on the ESXi host. For details, see the *vSphere Virtual Machine Administration* document.

Procedure

1. In vSphere Client, log in to the vCenter Server system where the virtual machine resides.
2. Right-click the virtual machine, select **Power**, and select **Power On** to start the virtual machine.
3. Right-click the virtual machine, select **Guest**, and select **Install/Upgrade VMware Tools** to install the latest version of VMware Tools.

   NOTE The virtual printing feature is supported only when you install it from Horizon Agent. Virtual printing is not supported if you install it with VMware Tools.

4. Ensure that the virtual machine is synchronized to a reliable time source.

   In general, guests can use the VMware Tools time synchronization method in preference to other methods of time synchronization. The VMware Tools online help provides information on configuring time synchronization between guest and host.

   A Windows guest that is a member of a Windows domain synchronizes its time with its domain controller using the Windows Time Service. For these guests, this is the appropriate time synchronization method and VMware Tools time synchronization must not be used.

   Guests must use only one method of time synchronization. For example, a Windows guest that is not a member of a Windows domain must have its Windows Time Service disabled.

   IMPORTANT Hosts that are being relied upon for time synchronization must themselves be synchronized to a reliable time source, using the built-in NTP client. Verify that all hosts in a cluster use the same time source.

   NOTE Windows domain controllers can use either VMware Tools time synchronization or another reliable time source. All domain controllers within a forest and domain controllers across forests with inter-forest trusts must be configured to use the same time source.

5. Install service packs and updates.
6. Install antivirus software.
7. Install other applications and software, such as smart card drivers if you are using smart card authentication.

   If you plan to use VMware Identity Manager to offer a catalog that includes ThinApp applications, you must install VMware Identity Manager for Windows.

   IMPORTANT If you are installing Microsoft .NET Framework, you must install it after you install Horizon Agent.

8 If Horizon Client devices will connect to the virtual machine with the PCoIP display protocol, set the power option **Turn off the display** to **Never**.

   If you do not disable this setting, the display will appear to freeze in its last state when power savings mode starts.

9 If Horizon Client devices will connect to the virtual machine with the PCoIP display protocol, go to **Control Panel > System > Advanced System Settings > Performance Settings** and change the setting for **Visual Effects** to **Adjust for best performance**.

   If you instead use the setting called **Adjust for best appearance** or **Let Windows choose what's best for my computer** and Windows chooses appearance instead of performance, performance is negatively affected.

10 If a proxy server is used in your network environment, configure network proxy settings.

11 Configure network connection properties.

   a Assign a static IP address or specify that an IP address is assigned by a DHCP server.

      View does not support link-local (169.254.x.x) addresses for View desktops.

   b Set the preferred and alternate DNS server addresses to your Active Directory server address.

12 (Optional) Join the virtual machine to the Active Directory domain for your remote desktops.

   A parent virtual machine for creating instant clones or View Composer linked clones must either belong to the same Active Directory domain as the domain that the desktop machines will join or be a member of a workgroup.

13 Configure Windows Firewall to allow Remote Desktop connections to the virtual machine.

14 (Optional) Disable Hot Plug PCI devices.

   This step prevents users from accidentally disconnecting the virtual network device (vNIC) from the virtual machine.

15 (Optional) Configure user customization scripts.

Prepare Windows Server Operating Systems for Desktop Use

To use a Windows Server 2008 R2 or Windows Server 2012 R2 virtual machine as a single-session View desktop (rather than as an RDS host), you must perform certain steps before you install Horizon Agent in the virtual machine. You must also configure View Administrator to treat Windows Servers as supported operating systems for View desktop use.

Prerequisites

- Familiarize yourself with the steps to install the Desktop Experience feature on Windows Server 2008 R2 or Windows Server 2012 R2. See "Install Desktop Experience on Windows Server 2008 R2," on page 25 or "Install Desktop Experience on Windows Server 2012 or 2012 R2," on page 26
- On Windows Server 2012 R2 machines, familiarize yourself with the steps to configure the Windows Firewall service to restart after failures occur. See "Configure the Windows Firewall Service to Restart After Failures," on page 26.

Procedure

1 Verify that the Remote Desktop Services role is not installed.

   When the Remote Desktop Services role is not present, the Horizon Agent installer prompts you to confirm that you want to install Horizon Agent in desktop mode. If the Remote Desktop Services role is present, the Horizon Agent installer does not display this prompt and it treats the Windows Server machine as an RDS host instead of a single-session View desktop.

2. Install Windows Server 2008 R2 Service Pack 1 (SP1) or Windows Server 2012 R2.

   If you do not install SP1 with Windows Server 2008 R2, an error occurs when you install Horizon Agent.

3. (Optional) Install the Desktop Experience feature if you plan to use the following features.

   - HTML Access
   - Scanner redirection
   - Windows Aero

4. (Optional) To use Windows Aero on a Windows Server desktop, start the Themes service.

   When you create or edit a desktop pool, you can configure 3D graphics rendering for your desktops. The 3D Renderer setting offers a Software option that enables users to run Windows Aero on the desktops in the pool.

5. On Windows Server 2012 R2 machines, configure the Windows Firewall service to restart after failures occur.

6. Configure View Administrator to treat Windows Servers as supported desktop operating systems.

   If you do not perform this step, you cannot select Windows Server machines for desktop use in View Administrator.

   a. In View Administrator, select **View Configuration > Global Settings**.

   b. In the General pane, click **Edit**.

   c. Select the **Enable Windows Server desktops** check box and click **OK**.

When you enable Windows Server desktops in View Administrator, View Administrator displays all available Windows Server machines, including machines on which View Connection Server is installed, as potential machines for desktop use. You cannot install Horizon Agent on machines on which other View software components are installed.

Install Desktop Experience on Windows Server 2008 R2

For RDS desktops and applications, and for VDI desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Procedure

1. Log in as an administrator.
2. Start Server Manager.
3. Click **Features**.
4. Click **Add Features**.
5. On the Select Features page, select the **Desktop Experience** checkbox.
6. Review the information about other features that are required by the Desktop Experience feature, and click **Add Required Features**.
7. Follow the prompts and finish the installation.

Install Desktop Experience on Windows Server 2012 or 2012 R2

For RDS desktops and applications, and for VDI desktops that are deployed on single-user virtual machines that run Windows Server, scanner redirection requires that you install the Desktop Experience feature on the RDS hosts and the single-user virtual machines.

Windows Server 2012 and Windows Server 2012 R2 are supported on machines that are used as RDS hosts. Windows Server 2012 R2 is supported on single-user virtual machines.

Procedure

1 Log in as an administrator.

2 Start Server Manager.

3 Select **Add roles and features**.

4 On the Select Installation Type page, select **Role-based or feature-based installation**.

5 On the Select Destination Server page, select a server.

6 On the Select Server Roles page, accept the default selection and click **Next**.

7 On the Select Features page, under **User Interfaces and Infrastructure**, select **Desktop Experience**.

8 Follow the prompts and finish the installation.

Configure the Windows Firewall Service to Restart After Failures

Some Windows Server 2012 R2, Windows 8.1, and Windows 10 machines that are deployed as single-session desktops do not become available immediately after they are provisioned. This issue occurs when the Windows Firewall service does not restart after its timeout period expires. You can configure the Windows Firewall service on the parent or template virtual machine to ensure that all machines in a desktop pool become available.

If you encounter this issue during provisioning, the Windows event logs display the following error: `The Windows Firewall service terminated with the following service-specific error: This operation returned because the timeout period expired.`

This issue occurs on Windows Server 2012 R2, Windows 8.1, and Windows 10 machines. Other guest operating systems are not affected.

Procedure

1 On the Windows Server 2012 R2, Windows 8.1, or Windows 10 parent or template virtual machine from which you will deploy a desktop pool, select **Control Panel > Administrative Tools > Services**.

2 In the Services dialog box, right-click the **Windows Firewall** service and select **Properties**.

3 In the Windows Firewall Properties dialog box, click the **Recovery** tab.

4 Select the recovery settings to restart the service after a failure occurs.

Setting	Drop-down Menu Option
First failure:	**Restart the Service**
Second failure:	**Restart the Service**
Subsequent failures:	**Restart the Service**

5 Select the **Enable actions for stops with errors** check box and click **OK**.

6 Deploy or redeploy the desktop pool from the parent or template virtual machine.

Install Horizon Agent on a Virtual Machine

You must install Horizon Agent on virtual machines that are managed by vCenter Server so that Connection Server can communicate with them. Install Horizon Agent on all virtual machines that you use as templates for full-clone desktop pools, parents for linked-clone desktop pools, parents for instant-clone desktop pools, and machines in manual desktop pools.

To install Horizon Agent on multiple Windows virtual machines without having to respond to wizard prompts, you can install Horizon Agent silently. See "Install Horizon Agent Silently," on page 30.

The Horizon Agent software cannot coexist on the same virtual or physical machine with other Horizon software components, including security server, Connection Server, and View Composer. It can coexist with Horizon Client.

Prerequisites

- Prepare the guest operating system for remote desktop deployment. See "Prepare a Guest Operating System for Remote Desktop Deployment," on page 22.
- To use a Windows Server virtual machine as a remote desktop (rather than as an RDS host), perform the steps described in "Prepare Windows Server Operating Systems for Desktop Use," on page 24.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at http://www.vmware.com/go/downloadview.
- Verify that you have administrative rights on the virtual machine.
- Familiarize yourself with the Horizon Agent custom setup options. See "Horizon Agent Custom Setup Options," on page 28.
- Familiarize yourself with the TCP ports that the Horizon Agent installation program opens on the firewall. See the *View Architecture Planning* document for more information.

Procedure

1. To start the Horizon Agent installation program, double-click the installer file.

   The installer filename is `VMware-viewagent-`*`y.y.y-xxxxxx`*`.exe` or `VMware-viewagent-x86_64-`*`y.y.y-xxxxxx`*`.exe`, where *y.y.y* is the version number and *xxxxxx* is the build number.

2. Accept the VMware license terms.

3. If you install Horizon Agent on a Windows Server machine on which the Remote Desktop Services (RDS) role is not installed, select **Install VMware Horizon Agent in 'desktop mode'**.

   Selecting this option configures the Windows Server machine as a single-user View desktop rather than as an RDS host. If you intend the machine to function as an RDS host, cancel the Horizon Agent installation, install the RDS role on the machine, and restart the Horizon Agent installation.

4. Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

   You must install all View components with the same IP version.

5. Select whether to enable or disable FIPS mode.

   This option is available only if FIPS mode is enabled in Windows.

6 Select your custom setup options.

To deploy View Composer linked-clone desktops, select the **VMware Horizon View Composer Agent** option. To deploy instant-clone desktops, select the **VMware Horizon Instant Clone Agent** option. You cannot select both of these options.

7 Accept or change the destination folder.

8 Follow the prompts in the Horizon Agent installation program and finish the installation.

Note If you did not enable Remote Desktop support during guest operating system preparation, the Horizon Agent installation program prompts you to enable it. If you do not enable Remote Desktop support during Horizon Agent installation, you must enable it manually after the installation is finished.

9 If you selected the USB redirection option, restart the virtual machine to enable USB support.

In addition, the **Found New Hardware** wizard might start. Follow the prompts in the wizard to configure the hardware before you restart the virtual machine.

What to do next

If the virtual machine has multiple NICs, configure the subnet that Horizon Agent uses. See "Configure a Virtual Machine with Multiple NICs for Horizon Agent," on page 36.

Horizon Agent Custom Setup Options

When you install Horizon Agent on a virtual machine, you can select or deselect custom setup options. In addition, Horizon Agent installs certain features automatically on all guest operating systems on which they are supported. These features are not optional.

To learn which features are supported on which guest operating systems, see "Feature Support Matrix for Horizon Agent" in the *View Architecture Planning* document.

To change custom setup options after you install the latest Horizon Agent version, you must uninstall and reinstall Horizon Agent. For patches and upgrades, you can run the new Horizon Agent installer and select a new set of options without uninstalling the previous version.

All custom setup options are selected by default except Serial Port Redirection, Scanner Redirection, USB Redirection, Flash Redirection, Smartcard Redirection, and VMware Horizon Instant Clone Agent.

Table 4-2. Horizon Agent Custom Setup Options in an IPv4 Environment

Option	Description
Core	Installs the core functionality.
Serial Port Redirection	Redirects serial COM ports that are connected to the client system so that they can be used on the remote desktop. This option is not selected by default. You must select the option to install it. Serial port redirection is supported on remote desktops that are deployed on single-user machines. Serial port redirection is available in Horizon 6 version 6.1.1 and later releases.
Scanner Redirection	Redirects scanning and imaging devices that are connected to the client system so that they can be used on the remote desktop or application. This option is not selected by default. You must select the option to install it. Scanner redirection is available in Horizon 6.0.2 and later releases.

Table 4-2. Horizon Agent Custom Setup Options in an IPv4 Environment (Continued)

Option	Description
USB Redirection	Gives users access to locally connected USB devices on their desktops. USB redirection is supported on remote desktops that are deployed on single-user machines. In addition, redirection of USB flash drives and hard disks is supported on RDS desktops and applications. This option is not selected by default. You must select the option to install it. For guidance on using USB redirection securely, see the *View Security* guide. For example, you can use group policy settings to disable USB redirection for specific users.
VMware Horizon View Composer Agent	Lets this virtual machine be the parent VM of a View Composer linked-clone desktop pool. If you select this option, you cannot select the **VMware Horizon Instant Clone Agent** option.
VMware Horizon Instant Clone Agent	Lets this virtual machine be the parent VM of an instant-clone desktop pool. This option is not selected by default. If you select this option, you cannot select the **VMware Horizon View Composer Agent** option.
Real-Time Audio-Video	Redirects webcam and audio devices that are connected to the client system so that they can be used on the remote desktop.
Client Drive Redirection	Allows Horizon Client users to share local drives with their remote desktops. After this option is installed, no further configuration is required on the remote desktop. Client Drive Redirection is also supported on RDS desktops and applications and on VDI desktops that run on unmanaged machines.
Virtual Printing	Lets users print to any printer available on their client computers. Users do not have to install additional drivers on their desktops. Virtual printing is supported on the following remote desktops and applications: ■ Desktops that are deployed on single-user machines, including Windows desktop and Windows Server machines. ■ Desktops that are deployed on RDS hosts, where the RDS hosts are virtual machines. ■ Remote applications. ■ Remote applications that are launched from Horizon Client inside remote desktops (nested sessions). The virtual printing feature is supported only when you install it from Horizon Agent. It is not supported if you install it with VMware Tools.
vRealize Operations Desktop Agent	Provides information that allows vRealize Operations for View to monitor View desktops.
View Persona Management	Synchronizes the user profile on the local desktop with a remote profile repository, so that users have access to their profiles whenever they log in to a desktop.
Smartcard Redirection	Lets users authenticate with smart cards when they use the PCoIP or Blast Extreme display protocol. This option is not selected by default. Smartcard Redirection is supported on remote desktops that are deployed on single-user machines.
VMware Audio	Provides a virtual audio driver on the remote desktop.
Flash Redirection	Redirects Flash multimedia content in an Internet Explorer 9, 10, or 11 browser to the client, for performance optimization. In Horizon 7.0, this is a Tech Preview feature. In Horizon 7.0.1, this feature is fully supported.

In an IPv6 environment, the only optional features are VMware Horizon View Composer Agent, VMware Horizon Instant Clone Agent, and VMware Audio.

Table 4-3. Horizon Agent Features That Are Installed Automatically (Not Optional)

Feature	Description
PCoIP Agent	Lets users connect to the View desktop using the PCoIP display protocol. Installing the PCoIP Agent feature disables sleep mode on Windows desktops. When a user navigates to the Power Options or Shut Down menu, sleep mode or standby mode is inactive. Desktops do not go into sleep or standby mode after a default period of inactivity. Desktops remain in active mode.
Windows Media Multimedia Redirection (MMR)	Extends multimedia redirection to Windows 7 and later desktops and clients. This feature delivers a multimedia stream directly to the client computer, allowing the multimedia stream to be processed on the client hardware instead of the remote ESXi host.
Unity Touch	Allows tablet and smart phone users to interact easily with Windows applications that run on the remote desktop. Users can browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications, all without using the Start menu or Taskbar.
Virtual video driver	Provides a virtual video driver on the remote desktop.

In an IPv6 environment, the only automatically installed feature is PCoIP Agent.

Install Horizon Agent Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install Horizon Agent on several Windows virtual machines or physical computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

With silent installation, you can efficiently deploy View components in a large enterprise.

If you do not want to install all features that are installed automatically or by default, you can use the `ADDLOCAL` MSI property to selectively install individual setup options and features. For details about the `ADDLOCAL` property, see Table 4-5.

Prerequisites

- Prepare the guest operating system for desktop deployment. See "Prepare a Guest Operating System for Remote Desktop Deployment," on page 22.
- To use Windows Server as a single-session remote desktop (rather than as an RDS host), perform the steps described in "Prepare Windows Server Operating Systems for Desktop Use," on page 24.
- If the machine has the Microsoft Visual C++ Redistributable package installed, verify that the version of the package is 2005 SP1 or later. If the package version is 2005 or earlier, you can either upgrade or uninstall the package.
- Download the Horizon Agent installer file from the VMware product page at http://www.vmware.com/go/downloadview.

  The installer filename is `VMware-viewagent-`*`y.y.y-xxxxxx`*`.exe` or `VMware-viewagent-x86_64-`*`y.y.y-xxxxxx`*`.exe`, where *y.y.y* is the version number and *xxxxxx* is the build number.
- Verify that you have administrative rights on the virtual machine or physical PC.
- Familiarize yourself with the Horizon Agent custom setup options. See "Horizon Agent Custom Setup Options," on page 28.

- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 31.
- Familiarize yourself with the silent installation properties available with Horizon Agent. See "Silent Installation Properties for Horizon Agent," on page 33.
- Familiarize yourself with the TCP ports that the Horizon Agent installation program opens on the firewall. See the *View Architecture Planning* document for more information.
- Verify that the latest Windows Update patches are installed on the guest operating systems on which you plan to install Horizon Agent silently. In certain cases, an interactive installation by an administrator might be required to execute pending Windows Update patches. Verify that all OS operations and subsequent reboots are completed.

Procedure

1 Open a Windows command prompt on the virtual machine or physical PC.

2 Type the installation command on one line.

The following example installs Horizon Agent with the components Core, VMware Blast, PCoIP, Unity Touch, VmVideo, PSG, View Composer Agent, Virtual Printing, USB redirection, and Real-Time Audio-Video components.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1
ADDLOCAL=Core,SVIAgent,ThinPrint,USB,RTAV"
```

The following example installs Horizon Agent on an unmanaged computer and registers the desktop with the specified View Connection Server, `cs1.companydomain.com`. In addition, the installer installs the Core, VMware Blast, PCoIP, Unity Touch, VmVideo, PSG, Virtual Printing, and USB redirection components.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=0
VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_USERNAME=admin.companydomain.com
VDM_SERVER_PASSWORD=secret ADDLOCAL=Core,ThinPrint,USB"
```

If you install Horizon Agent on a Windows Server machine, and you intend to configure the machine as a single-user View desktop rather than as an RDS host, you must include the `VDM_FORCE_DESKTOP_AGENT=1` property in the installation command. This requirement applies to machines that are managed by vCenter Server and unmanaged machines.

What to do next

If the virtual machine has multiple NICs, configure the subnet that Horizon Agent uses. See "Configure a Virtual Machine with Multiple NICs for Horizon Agent," on page 36.

Microsoft Windows Installer Command-Line Options

To install View components silently, you must use Microsoft Windows Installer (MSI) command-line options and properties. The View component installers are MSI programs and use standard MSI features.

For details about MSI, see the Microsoft Web site. For MSI command-line options, see the Microsoft Developer Network (MSDN) Library Web site and search for MSI command-line options. To see MSI command-line usage, you can open a command prompt on the View component computer and type `msiexec /?`.

To run a View component installer silently, you begin by silencing the bootstrap program that extracts the installer into a temporary directory and starts an interactive installation.

At the command line, you must enter command-line options that control the installer's bootstrap program.

Table 4-4. Command-Line Options for a View Component's Bootstrap Program

Option	Description
`/s`	Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs. For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s` The `/s` option is required to run a silent installation.
`/v"` *`MSI_command_line_options`*`"`	Instructs the installer to pass the double-quote-enclosed string that you enter at the command line as a set of options for MSI to interpret. You must enclose your command-line entries between double quotes. Place a double quote after the `/v` and at the end of the command line. For example: `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"command_line_options"` To instruct the MSI installer to interpret a string that contains spaces, enclose the string in two sets of double quotes. For example, you might want to install the View component in an installation path name that contains spaces. For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""` In this example, the MSI installer passes on the installation-directory path and does not attempt to interpret the string as two command-line options. Note the final double quote that encloses the entire command line. The `/v"command_line_options"` option is required to run a silent installation.

You control the remainder of a silent installation by passing command-line options and MSI property values to the MSI installer, `msiexec.exe`. The MSI installer includes the View component's installation code. The installer uses the values and options that you enter in the command line to interpret installation choices and setup options that are specific to the View component.

Table 4-5. MSI Command-Line Options and MSI Properties

MSI Option or Property	Description
`/qn`	Instructs the MSI installer not to display the installer wizard pages. For example, you might want to install Horizon Agent silently and use only default setup options and features: `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"` Alternatively, you can use the `/qb` option to display the wizard pages in a noninteractive, automated installation. As the installation proceeds, the wizard pages are displayed, but you cannot respond to them. The `/qn` or `/qb` option is required to run a silent installation.
`INSTALLDIR`	Specifies an alternative installation path for the View component. Use the format *`INSTALLDIR=path`* to specify an installation path. You can ignore this MSI property if you want to install the View component in the default path. This MSI property is optional.

Table 4-5. MSI Command-Line Options and MSI Properties (Continued)

MSI Option or Property	Description
ADDLOCAL	Determines the component-specific options to install. In an interactive installation, the View installer displays custom setup options that you can select or deselect. In a silent installation, you can use the ADDLOCAL property to selectively install individual setup options by specifying the options on the command line. Options that you do not explicitly specify are not installed. In both interactive and silent installations, the View installer automatically installs certain features. You cannot use ADDLOCAL to control whether or not to install these non-optional features. Type ADDLOCAL=ALL to install all custom setup options that can be installed during an interactive installation, including those that are installed by default and those that you must select to install, except NGVC. NGVC and SVIAgent are mutually exclusive. The following example installs Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and all features that are supported on the guest operating system: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" If you do not use the ADDLOCAL property, the custom setup options that are installed by default and the automatically installed features are installed. Custom setup options that are off (unselected) by default are not installed. The following example installs Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and the on-by-default custom setup options that are supported on the guest operating system: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn" To specify individual setup options, type a comma-separated list of setup option names. Do not use spaces between names. Use the format ADDLOCAL=*value*,*value*,*value*.... You must include Core when you use the ADDLOCAL=*value*,*value*,*value*... property. The following example installs Horizon Agent with the Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, Instant Clone Agent, and Virtual Printing features: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,NGVC,ThinPrint" The preceding example does not install other components, even those that are installed by default interactively. The ADDLOCAL MSI property is optional.
REBOOT	You can use the REBOOT=ReallySuppress option to allow system configuration tasks to complete before the system reboots. This MSI property is optional.
/l*v *log_file*	Writes logging information into the specified log file with verbose output. For example: /l*v ""%TEMP%\vmmsi.log"" This example generates a detailed log file that is similar to the log generated during an interactive installation. You can use this option to record custom features that might apply uniquely to your installation. You can use the recorded information to specify installation features in future silent installations. The /l*v option is optional.

Silent Installation Properties for Horizon Agent

You can include specific properties when you silently install Horizon Agent from the command line. You must use a *PROPERTY*=*value* format so that Microsoft Windows Installer (MSI) can interpret the properties and values.

Table 4-6 shows the Horizon Agent silent installation properties that you can use at the command-line.

Table 4-6. MSI Properties for Silently Installing Horizon Agent

MSI Property	Description	Default Value
`INSTALLDIR`	The path and folder in which the Horizon Agent software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	`%ProgramFiles %\VMware\VMware View\Agent`
`RDP_CHOICE`	Determines whether to enable Remote Desktop Protocol (RDP) on the desktop. A value of 1 enables RDP. A value of 0 leaves the RDP setting disabled. This MSI property is optional.	1
`UNITY_DEFAULT_APPS`	Specifies a default list of default favorite applications that are displayed in the Unity Touch sidebar on a mobile device. This property was created to support the Unity Touch component. It is not a general MSI property. For information about configuring a default list of favorite applications and about the syntax and format to use with this property, see "Configure Favorite Applications Displayed by Unity Touch" in the *Configuring Remote Desktop Features in Horizon 7* guide. This MSI property is optional.	
`URL_FILTERING_ENABLED`	Specifies whether the URL Content Redirection feature is installed. A value of 1 installs the feature. You must then use group policy settings to configure which URLs to redirect. See "Configuring URL Content Redirection in the *Configuring Remote Desktop Features in Horizon 7* document. This MSI property is optional.	0
`VDM_VC_MANAGED_AGENT`	Determines whether vCenter Server manages the virtual machine on which Horizon Agent is installed. A value of 1 configures the desktop as a vCenter Server-managed virtual machine. A value of 0 configures the desktop as unmanaged by vCenter Server. This MSI property is required.	None
`VDM_SERVER_NAME`	The host name or IP address of the View Connection Server computer on which the Horizon Agent installer registers an unmanaged desktop. This property applies to unmanaged desktops only. For example: `VDM_SERVER_NAME=10.123.01.01` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual-machine desktops that are managed by vCenter Server.	None
`VDM_SERVER_USERNAME`	The user name of the administrator on the View Connection Server computer. This MSI property applies to unmanaged desktops only. For example: `VDM_SERVER_USERNAME=domain\username` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual-machine desktops that are managed by vCenter Server.	None
`VDM_SERVER_PASSWORD`	The View Connection Server administrator user password. For example: `VDM_SERVER_PASSWORD=secret` This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual-machine desktops that are managed by vCenter Server.	None

Table 4-6. MSI Properties for Silently Installing Horizon Agent (Continued)

MSI Property	Description	Default Value
`VDM_IP_PROTOCOL_USAGE`	Specifies the IP version that Horizon Agent uses. The possible values are IPv4 and IPv6.	IPv4
`VDM_FIPS_ENABLED`	Specifies whether to enable or disable FIPS mode. A value of 1 enables FIPS mode. A value of 0 disables FIPS mode. If this property is set to 1 and Windows is not in FIPS mode, the installer will abort.	0
`VDM_FLASH_URL_REDIRECTION`	Determines whether Horizon Agent can install the Flash URL redirection feature. Specify 1 to enable installation or 0 to disable installation. This MSI property is optional.	0

In a silent installation command, you can use the MSI property, `ADDLOCAL=`, to specify options that the Horizon Agent installer configures.

Table 4-7 shows the Horizon Agent options you can type at the command line. These options have corresponding setup options that you can deselect or select during an interactive installation. For details about the custom setup options, see "Horizon Agent Custom Setup Options," on page 28.

When you do not use the `ADDLOCAL` property at the command line, Horizon Agent installs all options that are installed by default during an interactive installation, if they are supported on the guest operating system. When you use `ADDLOCAL=ALL`, Horizon Agent installs all of the following options, both on-by-default and off-by-default, if they are supported on the guest operating system, except NGVC. NGVC and SVIAgent are mutually exclusive. To install NGVC, you must specify it explicitly. For details, see the `ADDLOCAL` table entry in "Microsoft Windows Installer Command-Line Options," on page 31.

Table 4-7. Horizon Agent Silent Installation Options and Interactive Custom Setup Options

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When `ADDLOCAL` Is Not Used
Core	Core	Yes
USB	USB Redirection	No
SVIAgent	View Composer Agent	Yes
NGVC	Instant Clone Agent	No
RTAV	Real-Time Audio-Video	Yes
ClientDriveRedirection	Client Drive Redirection	Yes
SerialPortRedirection	Serial Port Redirection	No
ScannerRedirection	Scanner Redirection	No
FlashURLRedirection	Flash URL Redirection This feature is hidden unless you use the `VDM_FLASH_URL_REDIRECTION=1` property on the command line.	No
ThinPrint	Virtual Printing	Yes
V4V	vRealize Operations Desktop Agent	Yes
VPA	View Persona Management	Yes
SmartCard	PCoIP Smartcard. This feature is not installed by default in an interactive installation.	No
VmwVaudio	VMware Audio (virtual audio driver)	Yes

Table 4-7. Horizon Agent Silent Installation Options and Interactive Custom Setup Options (Continued)

Silent Installation Option	Custom Setup Option in an Interactive Installation	Installed by Default Interactively or When `ADDLOCAL` Is Not Used
TSMMR	Windows Media Multimedia Redirection (MMR)	Yes
RDP	This feature enables RDP in the registry if you use the `RDP_CHOICE=1` property on the command line or select RDP as the default display protocol when you create or edit a desktop pool in View Administrator. This feature is hidden during interactive installations.	Yes

If you use `ADDLOCAL` to specify features individually, that is, you do not specify `ADDLOCAL=ALL`, you must always specify `Core`.

Table 4-8. Horizon Agent Silent Installation Features That Are Installed Automatically

Silent Installation Feature	Description
Core	The core Horizon Agent functions. If you specify `ADDLOCAL=ALL`, the Core features are installed.
BlastProtocol	VMware Blast
PCoIP	PCoIP Protocol Agent
VmVideo	Virtual video driver
UnityTouch	Unity Touch
PSG	This features sets a registry entry that tells Connection Server whether Horizon Agent is using IPv4 or IPv6.

You install the Flash URL Redirection feature by using the `VDM_FLASH_URL_REDIRECTION=1` property in a silent installation. This feature is not installed during an interactive installation or by using `ADDLOCAL=ALL` in a silent installation.

For example: `VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1 VDM_FLASH_URL_REDIRECTION=1 ADDLOCAL=Core,SVIAgent,ThinPrint,USB,FlashURLRedirection,RTAV"`

Configure a Virtual Machine with Multiple NICs for Horizon Agent

When you install Horizon Agent on a virtual machine that has more than one NIC, you must configure the subnet that Horizon Agent uses. The subnet determines which network address Horizon Agent provides to the Connection Server instance for client protocol connections.

Procedure

◆ On the virtual machine on which Horizon Agent is installed, open a command prompt, type **`regedit.exe`**, and create a registry entry to configure the subnet.

  For example, in an IPv4 network:
  `HKLM\Software\VMware, Inc.\VMware VDM\IpPrefix = `*`n.n.n.n/m`*` (REG_SZ)`

  In this example, *n.n.n.n* is the TCP/IP subnet and *m* is the number of bits in the subnet mask.

  NOTE In releases earlier than Horizon 6 version 6.1, this registry path was **`HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = `*`n.n.n.n/m`*` (REG_SZ)`**. The old registry setting is not used with View Agent 6.1 or later. If you upgrade View Agent from an earlier release to version 6.1 or later, make sure to use the current registry setting.

Optimize Guest Operating System Performance

You can perform certain steps to optimize guest operating system performance for remote desktop deployment. All of the steps are optional.

These recommendations include turning off the screen saver and not specifying a sleep timer. Your organization might require the use of screen savers. For example, you might have a GPO-managed security policy that locks a desktop a certain time after the screen saver starts. In this case, use a blank screen saver.

Prerequisites

- Prepare a guest operating system for remote desktop deployment.
- Familiarize yourself with the procedure for disabling the Windows Customer Experience Improvement Program. See "Disable the Windows Customer Experience Improvement Program," on page 38.

Procedure

- Disable any unused ports, such as COM1, COM2, and LPT.
- Adjust display properties.
  a Choose a basic theme.
  b Set the background to a solid color.
  c Set the screen saver to **None**.
  d Verify that hardware acceleration is enabled.
- Select a high-performance power option and do not specify a sleep timer.
- Disable the Indexing Service component.

  NOTE Indexing improves searches by cataloging files. Do not disable this feature for users who search often.

- Remove or minimize System Restore points.
- Turn off system protection on `C:\`.
- Disable any unnecessary services.
- Set the sound scheme to **No Sounds**.
- Set visual effects to **Adjust for best performance**.
- Open Windows Media Player and use the default settings.
- Turn off automatic computer maintenance.
- Adjust performance settings for best performance.
- Delete any hidden uninstall folders in `C:\Windows`, such `$NtUninstallKB893756$`.
- Delete all event logs.
- Run Disk Cleanup to remove temporary files, empty the Recycle Bin, and remove system files and other items that are no longer needed.
- Run Disk Defragmenter to rearrange fragmented data.
- Uninstall Tablet PC Components, unless this feature is needed.
- Disable IPv6, unless it is needed.

- Use the File System Utility (`fsutil`) command to disable the setting that keeps track of the last time a file was accessed.

  For example: `fsutil behavior set disablelastaccess 1`

- Start the Registry Editor (`regedit.exe`) and change the **TimeOutValue** REG_DWORD in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk` to **`0x000000be(190)`**.

- Turn off the Windows Customer Experience Improvement Program and disable related tasks from the Task Scheduler.

- Restart Windows after you make the above changes.

What to do next

See "Optimizing Windows for Instant-Clone and View Composer Linked-Clone Virtual Machines," on page 39 for information on disabling certain Windows services and tasks to reduce the growth of instant clones and View Composer linked clones. Disabling certain services and tasks can also result in performance benefits for full virtual machines.

Disable the Windows Customer Experience Improvement Program

Disabling the Windows Customer Experience Improvement Program and the related Task Scheduler tasks that control this program can improve Windows 7, Windows 8/8.1, and Windows 10 system performance in large desktop pools.

The following steps apply to Windows 7 and Windows 8. The steps might vary on different Windows operating systems.

Procedure

1. In the Windows 7 or Windows 8 guest operating system, start the control panel and click **Action Center > Change Action Center settings**.
2. Click **Customer Experience Improvement Program settings**.
3. Select **No, I don't want to participate in the program** and click **Save changes**.
4. Start the control panel and click **Administrative Tools > Task Scheduler**.
5. In the Task Scheduler (Local) pane of the Task Scheduler dialog box, expand the **Task Scheduler Library > Microsoft > Windows** nodes and open the **Application Experience** folder.
6. Disable the **AITAgent**, **ProgramDataUpdater**, and if available, **Microsoft Compatibility Appraiser** tasks.
7. In the **Task Scheduler Library > Microsoft > Windows** node, open the **Customer Experience Improvement Program** folder.
8. Disable the **Consolidator**, **KernelCEIPTask**, and **UsbCEIP** tasks.
9. In the **Task Scheduler Library > Microsoft > Windows** node, open the **Autochk** folder.
10. Disable the **Proxy** task.

What to do next

Perform other Windows optimization tasks. See "Optimize Guest Operating System Performance," on page 37.

Optimizing Windows for Instant-Clone and View Composer Linked-Clone Virtual Machines

By disabling certain Windows 7, Windows 8/8.1, and Windows 10 services and tasks, you can reduce the growth in disk usage of instant clones and View Composer linked clones. Disabling certain services and tasks can also result in performance benefits for full virtual machines.

Benefits of Disabling Windows Services and Tasks

Windows 7, Windows 8/8.1, and Windows 10 schedule services and tasks that can cause instant clones and View Composer linked clones to grow, even when the machines are idle. The incremental growth of the OS disk can undo the storage savings that you achieve when you first create the clones. You can reduce growth in disk size by disabling these Windows services.

Windows guest operating systems schedule services such as disk defragmentation to run by default. These services run in the background if you do not disable them.

Services that affect OS disk growth also generate input/output operations. Disabling these services can reduce IOPS (input/output operations per second) and improve performance for any type of desktop machines.

These best practices for optimizing Windows apply to most user environments. However, you must evaluate the effect of disabling each service on your users, applications, and desktops. You might require certain services to stay active.

For example, disabling Windows Update Service makes sense for instant clones because the OS is refreshed each time a user logs off, and for View Composer linked clones if you refresh or recompose regularly.

Windows Services and Tasks That Cause Disk Growth in Instant Clones and Linked Clones

Certain services and tasks in Windows 7, Windows 8/8.1, and Windows 10 can cause the OS disk of an instant clone or a View Composer linked clone to grow incrementally, even when the machine is idle. If you disable these services and tasks, you can control the OS disk growth.

Services that affect OS disk growth also generate I/O operations. You can evaluate the benefits of disabling these services for full clones as well.

Before you disable the Windows services that are shown in Table 4-9, verify that you took the optimization steps in “Optimize Guest Operating System Performance,” on page 37.

Table 4-9. Impact of Windows Services and Tasks on OS Disk Growth and IOPS

Service or Task	Description	Default Occurrence or Startup	Impact on OS Disk	Impact on IOPS	Turn Off This Service or Task?
Windows Hibernation	Provides a power-saving state by storing open documents and programs in a file before the computer is powered off. The file is reloaded into memory when the computer is restarted, restoring the state when the hibernation was invoked.	Default power-plan settings disable hibernation.	High. By default, the size of the hibernation file, `hiberfil.sys`, is the same as the installed RAM on the virtual machine. This feature affects all guest operating systems.	High. When hibernation is triggered, the system writes a `hiberfil.sys` file the size of the installed RAM.	Yes Hibernation provides no benefit in a virtual environment. For instructions, see "Disable Windows Hibernation in the Parent Virtual Machine," on page 47.
Windows Scheduled Disk Defragmentation	Disk defragmentation is scheduled as a background process.	Once a week	High. Repeated defragmentation operations can increase the size of the OS disk by several GB and do little to make disk access more efficient .	High	Yes
Windows Update Service	Detects, downloads, and installs updates for Windows and other programs.	Automatic startup	Medium to high. Causes frequent writes to the OS disk because update checks occur often. The impact depends on the updates that are downloaded.	Medium to high	Yes, for instant clones, and for View Composer linked clones that you refresh or recompose regularly.
Windows Diagnostic Policy Service	Detects, troubleshoots, and resolves problems in Windows components. If you stop this service, diagnostics no longer function.	Automatic startup	Medium to high. The service is triggered on demand. The write frequency varies, depending on demand.	Small to medium	Yes, if you do not need the diagnostic tools to function on the desktops.
Prefetch/Superfetch	Stores specific information about applications that you run to help them start faster.	Always on, unless it is disabled.	Medium Causes periodic updates to its layout and database information and individual prefetch files, which are generated on demand.	Medium	Yes, if application startup times are acceptable after you disable this feature.

Table 4-9. Impact of Windows Services and Tasks on OS Disk Growth and IOPS (Continued)

Service or Task	Description	Default Occurrence or Startup	Impact on OS Disk	Impact on IOPS	Turn Off This Service or Task?
Windows Registry Backup (`RegIdleBackup`)	Automatically backs up the Windows registry when the system is idle.	Every 10 days at 12:00 am	Medium. Each time this task runs, it generates registry backup files.	Medium.	Yes. Both instant clones and View Composer linked clones let you revert to a snapshot and achieve the goal of restoring the registry.
System Restore	Reverts the Windows system to a previous, healthy state.	When Windows starts up and once a day thereafter.	Small to medium. Captures a system restore point whenever the system detects that it is needed.	No major impact.	Yes. Both instant clones and View Composer linked clones let you revert to a healthy state.
Windows Defender	Provides anti-spyware features.	When Windows starts up. Performs a quick scan once a day. Checks for updates before each scan.	Medium to high. Performs definition updates, scheduled scans, and scans that are started on demand.	Medium to high.	Yes, if other anti-spyware software is installed.
Microsoft Feeds Synchronization task (`msfeedssync.exe`)	Periodically updates RSS feeds in Windows Internet Explorer Web browsers. This task updates RSS feeds that have automatic RSS feeds synchronization turned on. The process appears in Windows Task Manager only when Internet Explorer is running.	Once a day.	Medium. Affects OS-disk growth if persistent disks are not configured. If persistent disks are configured, the impact is diverted to the persistent disks.	Medium	Yes, if your users do not require automatic RSS feed updates on their desktops.

Disable Scheduled Disk Defragmentation on a Windows Parent Virtual Machine

When you prepare a parent virtual machine for instant clones or View Composer linked clones, it is recommended that you disable scheduled defragmentation. Windows schedule weekly disk defragmentations by default. Defragmentation significantly increase the size of a clone's virtual disk and does not make disk access more efficient for instant clones or View Composer linked clones.

The clones share the parent virtual machine's OS disk but each clone maintains changes to the file system in its own virtual disk. Any activity, including defragmentation, will increase the size of each clone's individual virtual disk and therefore increase storage consumption. As a best practice, defragment the parent virtual machine before you take a snapshot and create the pool.

The following steps apply to Windows 7 and Windows 8. The steps might vary on different Windows operating systems.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in as an administrator.

3 Click **Start** and type `defrag` in the **Search programs and files** box.

4 In the Programs pane, click **Disk Defragmenter**.

5 In the **Disk Defragmenter** dialog box, click **Defragment disk**.

The Disk Defragmenter consolidates defragmented files on the virtual machine's hard disk.

6 In the **Disk Defragmenter** dialog box, click **Configure schedule**.

7 Deselect **Run on a schedule (recommended)** and click **OK**.

Disable Windows Update

Disabling the Windows Update feature avoids some I/O operations to the file system and can reduce the growth of an instant clone's or a View Composer linked clone's virtual disk.

Evaluate the needs of your environment before disabling Windows Update. If you disable this feature, you can manually download the updates to the parent virtual machine and then use the push-image operation for instant clones or recompose for View Composer linked clones to apply the updates to all the clones.

The following steps apply to Windows 7 and Windows 8. The steps might vary on different Windows operating systems.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in as an administrator.

3 Click **Start > Control Panel > System and Security > Turn automatic updating on or off**.

4 In the Important updates menu, select **Never check for updates**.

5 Deselect **Give me recommended updates the same way I receive important updates**.

6 Deselect **Allow all users to install updates on this computer** and click **OK**.

Disable the Diagnostic Policy Service on Windows Virtual Machines

Disabling the Windows Diagnostic Policy Service avoids some I/O operations to the file system and can reduce the growth of an instant clone's or a View Composer linked clone's virtual disk.

Do no disable the Windows Diagnostic Policy Service if your users require the diagnostic tools on their desktops.

The following steps apply to Windows 7 and Windows 8. The steps might vary on different Windows operating systems.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in as an administrator.

3 Click **Start > Control Panel > System and Security > Administrative Tools**.

4 Select **Services** and click **Open**.

5 Double-click **Diagnostic Policy Service**.

6 In the Diagnostic Policy Service Properties (Local Computer) dialog, click **Stop**.

7 In the Startup type menu, select **Disabled**.

8 Click **OK**.

Disable the Prefetch and Superfetch Features on Windows Virtual Machines

Disabling the prefetch and superfetch features avoids some I/O operations to the file system and can reduce the growth of an instant clone's or a View Composer linked clone's virtual disk.

To disable the prefetch and superfetch features, you must edit a Windows registry key and disable the Prefetch service on the virtual machine.

The following steps apply to Windows 7 and Windows 8. The steps might vary on different Windows operating systems.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the Windows Registry Editor.

Procedure

1 Start the Windows Registry Editor on the local Windows virtual machine.

2 Navigate to the registry key called **PrefetchParameters**.

  The registry key is located in the following path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters`.

3 Set the **EnablePrefetcher** and **EnableSuperfetch** values to **`0`**.

4 Click **Start > Control Panel > System and Security > Administrative Tools**.

5 Select **Services** and click **Open**.

6 Double-click the **Superfetch** service.

7 In the Superfetch Properties (Local Computer) dialog, click **Stop**.

8 In the Startup type menu, select **Disabled**.

9 Click **OK**.

Disable Windows Registry Backup on Windows Virtual Machines

Disabling the Windows registry backup feature, `RegIdleBackup`, avoids some I/O operations to the file system and can reduce the growth of an instant clone's or a View Composer linked clone's virtual disk.

The following steps apply to Windows 7 and Windows 8. The steps might vary on different Windows operating systems.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in as an administrator.

3 Click **Start > Control Panel > System and Security > Administrative Tools**.

4 Select **Task Scheduler** and click **Open**.

5 In the left pane, expand **Task Scheduler Library**, **Microsoft**, **Windows**.

6 Double-click **Registry** and select **RegIdleBackup**.

7 In the Actions pane, click **Disable**.

Disable the System Restore on Windows Virtual Machines

Disabling the Windows System Restore feature avoids some I/O operations to the file system and can reduce the growth of an instant clone's or a View Composer linked clone's virtual disk.

With System Restore, you can revert a machine's state to a previous point in time. You can achieve the same result with the push image operation for instant clones and the recompose or refresh operation for View Composer linked clones. Furthermore, with instant clones, when a user logs off, the machine is recreated, making a system restore unnecessary

The following steps apply to Windows 7 and Windows 8. The steps might vary on different Windows operating systems.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in as an administrator.

3 Click **Start > Control Panel > System and Security > Administrative Tools**.

4 Select **Task Scheduler** and click **Open**.

5 In the left pane, expand **Task Scheduler Library**, **Microsoft**, **Windows**.

6 Double-click **SystemRestore** and select **SR**.

7 In the Actions pane, click **Disable**.

Disable Windows Defender on Windows Virtual Machines

Disabling Windows Defender avoids some I/O operations to the file system and can reduce the growth of an instant clone's or a View Composer linked clone's virtual disk.

If Windows Defender is the only anti-spyware installed on the virtual machine, you might prefer to keep Windows Defender active on the desktops in your environment.

The following steps apply to Windows 7 and Windows 8. The steps might vary on different Windows operating systems.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in as an administrator.

3 Click **Start** and type `Windows Defender` in the Search programs and files box.

4 Click **Tools > Options > Administrator**.

5 Deselect **Use this program** and click **Save**.

Disable Microsoft Feeds Synchronization on Windows Virtual Machines

Windows Internet Explorer uses the Microsoft Feeds Synchronization task to update RSS feeds in users' Web browsers. Disabling this task avoids some I/O operations to the file system and can reduce the growth of an instant clone's or a View Composer linked clone's virtual disk.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in as an administrator.

3 Click **Start > Control Panel > Network and Internet > Internet Options**.

4 Click the **Content** tab.

5 Under Feeds and Web Slices, click **Settings**.

6 Deselect **Automatically check feeds and Web Slices for updates** and click **OK**.

7 In the Internet Properties dialog, click **OK**.

Preparing a Parent Virtual Machine

To deploy an instant-clone or a View Composer linked-clone desktop pool, you must first prepare a parent virtual machine.

- Configure a Parent Virtual Machine on page 45

  After creating a virtual machine that you plan to use as a parent, configure the Windows environment.

- Activating Windows on Instant Clones and View Composer Linked Clones on page 47

  To make sure that Windows 7, Windows 8/8.1, Windows 10, and Windows Server clones are properly activated when the clones are created, you must use Microsoft volume activation on the parent virtual machine. The volume-activation technology requires a volume license key.

- Disable Windows Hibernation in the Parent Virtual Machine on page 47

  The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Disabling hibernation reduces the size of an instant clone's or a View Composer linked clone's virtual disk.

- Configure Local Storage for View Composer Linked Clones on page 48

  For a View Composer linked-clone desktop pool, you can configure the parent virtual machine to store virtual-machine swap files on a local datastore. The linked clones' swap files will reside on local storage. This feature is not available to instant clones.

- Record the Paging File Size of a View Composer Parent Virtual Machine on page 48

  When you create a View Composer linked-clone desktop pool, you can redirect the clones' paging and temp files to a separate disk. You must configure this disk to be larger than the size of the paging file on the parent virtual machine.

- Increase the Timeout Limit for ClonePrep and QuickPrep Customization Scripts on page 49

  ClonePrep and QuickPrep post-synchronization or power-off scripts have a timeout limit of 20 seconds. You can increase this limit by changing the `ExecScriptTimeout` Windows registry value on the parent virtual machine.

Configure a Parent Virtual Machine

After creating a virtual machine that you plan to use as a parent, configure the Windows environment.

Prerequisites

- Verify that you prepared a virtual machine to use for deploying remote desktops. See "Creating a Virtual Machine for Cloning," on page 19.

  The parent virtual machine can either belong to the same Active Directory domain as the domain that the desktop machines will join or be a member of a workgroup.

- Verify that the virtual machine was not converted from an instant clone or a View Composer linked clone.

  IMPORTANT You also cannot use an instant clone or a View Composer linked clones as a parent virtual machine.

- When you install Horizon Agent on the parent virtual machine, select the **VMware Horizon Instant Clone Agent** option for instant clones or the **VMware Horizon View Composer Agent** option. See "Install Horizon Agent on a Virtual Machine," on page 27.

  To update Horizon Agent in a large environment, you can use standard Windows update mechanisms such as Altiris, SMS, LanDesk, BMC, or other systems management software. You can also use the push image or the recompose operation to update Horizon Agent.

  Note For View Composer linked clones, do not change the log on account for the VMware View Composer Guest Agent Server service in a parent virtual machine. By default, this is the Local System account. If you change this account, the linked clones created from the parent will not start.

- To deploy Windows machines, configure a volume license key and activate the parent virtual machine's operating system with volume activation. See "Activating Windows on Instant Clones and View Composer Linked Clones," on page 47.
- Verify that you followed the best practices for optimizing the operating system. See "Optimizing Windows for Instant-Clone and View Composer Linked-Clone Virtual Machines," on page 39.
- Familiarize yourself with the procedure for disabling searching Windows Update for device drivers. See the Microsoft Technet article, "Disable Searching Windows Update for Device Drivers" at http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx.

Procedure

- Remove the DHCP lease on the parent virtual machine to avoid copying a leased IP address to the linked clones in the pool.

  a On the parent virtual machine, open a command prompt.

  b Type the **`ipconfig /release`** command.

- Verify that the system disk contains a single volume.

  You cannot deploy linked clones from a parent virtual machine that contains more than one volume. Multiple virtual disks are supported.

  Note For View Composer linked clones, if the parent virtual machine contains multiple virtual disks, when you create a desktop pool, do not select a drive letter for the View Composer persistent disk or disposable data disk that already exists on the parent virtual machine or that conflicts with a drive letter that is used for a network-mounted drive.

- Verify that the virtual machine does not contain an independent disk.

  An independent disk is excluded when you take a snapshot of the virtual machine. Clones are based on a snapshot and therefore will not contain the independent disk.

- For View Composer linked clones, if you plan to configure disposable data disks when you create linked-clone machines, remove default user `TEMP` and `TMP` variables from the parent virtual machine.

  You can also remove the `pagefile.sys` file to avoid duplicating the file on all the linked clones. If you leave the `pagefile.sys` file on the parent virtual machine, a read-only version of the file is inherited by the linked clones, while a second version of the file is used on the disposable data disk.

- Disable the hibernation option to reduce the size of each clone's virtual disk.
- Before you take a snapshot of the parent virtual machine, disable searching Windows Update for device drivers.

  This Windows feature can interfere with the customization process. As each clone is customized, Windows might search for the best drivers on the Internet for that clone, resulting in delays.

- In vSphere Client, disable the vApp Options setting on the parent virtual machine.

- On Windows 8.1, Windows Server 2008 R2, and Windows Server 2012 R2 machines, disable the scheduled maintenance task that recovers disk space by removing unused features.

  For example: `Schtasks.exe /change /disable /tn "\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"`

  For example, in the case of View Composer linked clones, this maintenance task can, remove the Sysprep customization script after the linked clones are created, which would cause subsequent recompose operations to fail with customization operation timeout errors. For more information, see the Microsoft KB article available at http://support.microsoft.com/kb/2928948.

What to do next

Use vSphere Client or vSphere Web Client to take a snapshot of the parent virtual machine in its powered-down state. This snapshot is provides the base image for the clones.

IMPORTANT Before you take a snapshot, shut down the parent virtual machine.

Activating Windows on Instant Clones and View Composer Linked Clones

To make sure that Windows 7, Windows 8/8.1, Windows 10, and Windows Server clones are properly activated when the clones are created, you must use Microsoft volume activation on the parent virtual machine. The volume-activation technology requires a volume license key.

To activate Windows with volume activation, you use Key Management Service (KMS), which requires a KMS license key. See your Microsoft dealer to acquire a volume license key and configure volume activation.

NOTE Multiple Activation Key (MAK) licensing is not supported.

Before you create an instant-clone or View Composer linked-clone desktop pool, you must use volume activation to activate Windows on the parent virtual machine.

The following steps describe how activation takes place:

1. Invoke a script to remove the existing license.
2. Restart Windows.
3. Invoke a script that uses KMS licensing to activate Windows.

KMS treats each activated clone as a computer with a newly issued license.

Disable Windows Hibernation in the Parent Virtual Machine

The Windows hibernation feature creates a hidden system file, `Hiberfil.sys` and uses this file to store information that is needed for hybrid sleep. Disabling hibernation reduces the size of an instant clone's or a View Composer linked clone's virtual disk.

⚠ **CAUTION** When you make hibernation unavailable, hybrid sleep does not work. Users can lose data if a power loss occurs.

Procedure

1. In vSphere Client, select the parent virtual machine and select **Open Console**.
2. Log in as an administrator.
3. Disable the hibernation option.
   a. Click **Start** and type **`cmd`** in the **Start Search** box.
   b. In the search results list, right-click **Command Prompt** and click **Run as Administrator**.

  c At the User Account Control prompt, click **Continue**.

  d At the command prompt, type `powercfg.exe /hibernate off` and press Enter.

  e Type `exit` and press Enter.

Configure Local Storage for View Composer Linked Clones

For a View Composer linked-clone desktop pool, you can configure the parent virtual machine to store virtual-machine swap files on a local datastore. The linked clones' swap files will reside on local storage. This feature is not available to instant clones.

In this procedure, you configure local storage for the virtual-machine swap files, not the paging and temp files in the guest OS. When you create a linked-clone pool, you also can redirect guest OS paging and temp files to a separate disk. See "Worksheet for Creating a Linked-Clone Desktop Pool," on page 61.

Procedure

1 Configure a swapfile datastore on the ESXi host or cluster on which you will deploy the linked-clone pool.

2 When you create the parent virtual machine in vCenter Server, store the virtual-machine swap files on the swapfile datastore on the local ESXi host or cluster:

  a In vSphere Client, select the parent virtual machine.

  b Click **Edit Settings** and click the **Options** tab.

  c Click **Swapfile location** and click **Store in the host's swapfile datastore**.

  For detailed instructions, see the VMware vSphere documentation.

Record the Paging File Size of a View Composer Parent Virtual Machine

When you create a View Composer linked-clone desktop pool, you can redirect the clones' paging and temp files to a separate disk. You must configure this disk to be larger than the size of the paging file on the parent virtual machine.

When a linked clone that is configured with a separate disk for the disposable files is powered off, the disk is recreated. This feature can slow the growth in the size of a linked clone. However, this feature can work only if you configure the disposable-file disk to be large enough to hold the clone's paging file.

Before you can configure the disposable-file disk, record the maximum paging-file size in the parent virtual machine. The linked clones have the same paging-file size as the parent virtual machine.

As a best practice, remove the `pagefile.sys` file from the parent virtual machine before you take a snapshot, to avoid duplicating the file on all the linked clones. See "Configure a Parent Virtual Machine," on page 45.

Note This feature is not that same as configuring local storage for the virtual-machine swap files. See "Configure Local Storage for View Composer Linked Clones," on page 48.

Procedure

1 In vSphere Client, right-click the parent virtual machine and click **Open Console**.

2 Select **Start** > **Settings** > **Control Panel** > **System**.

3 Click the **Advanced** tab.

4 In the Performance pane, click **Settings**.

5 Click the **Advanced** tab.

6 In the Virtual memory pane, click **Change**.

The Virtual Memory page appears.

7 Set the paging file size to a larger value than the size of the memory that is assigned to the virtual machine.

IMPORTANT If the **Maximum size (MB)** setting is smaller than the virtual-machine memory size, type a larger value and save the new value.

8 Keep a record of the **Maximum size (MB)** setting that is configured in the Paging file size for selected drive pane.

What to do next

When you configure a linked-clone pool from this parent virtual machine, configure a disposable-file disk that is larger than the paging-file size.

Increase the Timeout Limit for ClonePrep and QuickPrep Customization Scripts

ClonePrep and QuickPrep post-synchronization or power-off scripts have a timeout limit of 20 seconds. You can increase this limit by changing the `ExecScriptTimeout` Windows registry value on the parent virtual machine.

Instead of increasing the timeout limit you can also use your customization script to launch another script or process that performs the long-running task.

NOTE Most QuickPrep customization scripts can finish running within the 20-second limit. Test your scripts before you increase the limit.

Procedure

1 On the parent virtual machine, start the Windows Registry Editor.

a Select **Start > Command Prompt**.

b At the command prompt, type **regedit**.

2 In the Windows registry, locate the `vmware-viewcomposer-ga` registry key.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga
```

3 Click **Edit** and modify the registry value.

```
Value Name: ExecScriptTimeout
Value Type: REG_DWORD
Value unit: milliseconds
```

The default value is 20000 milliseconds.

Creating Virtual Machine Templates

You must create a virtual machine template before you can create an automated pool that contains full virtual machines.

A virtual machine template is a master copy of a virtual machine that can be used to create and provision new virtual machines. Typically, a template includes an installed guest operating system and a set of applications.

You create virtual machine templates in vSphere Client. You can create a virtual machine template from a previously configured virtual machine, or you can convert a previously configured virtual machine to a virtual machine template.

See the *vSphere Basic System Administration* guide for information on using vSphere Client to create virtual machine templates. See "Automated Pools That Contain Full Virtual Machines," on page 51 for information on creating automated pools.

Note A virtual machine template is not for creating an instant-clone or a View Composer linked-clone desktop pool.

Creating Customization Specifications

When you customize a clone using Sysprep, you need to provide a customization specification.

Sysprep is available for View Composer linked-clone desktop pools and automated full-clone desktop pools, but not instant-clone desktop pools. You create customization specifications by using the Customization Specification wizard in vSphere. See the *vSphere Virtual Machine Administration* document for information on using the Customization Specification wizard.

It is recommended that you test a customization specification in vSphere before you use it to create a desktop pool. When you use a Sysprep customization specification to join a Windows desktop to a domain, you must use the fully qualified domain name (FQDN) of the Active Directory domain. You cannot use the NetBIOS name.

Creating Automated Desktop Pools That Contain Full Virtual Machines 5

With an automated desktop pool that contains full virtual machines, you create a virtual machine template and View uses that template to create virtual machines for each desktop. You can optionally create customization specifications to expedite automated pool deployments.

This chapter includes the following topics:

Automated Pools That Contain Full Virtual Machines

To create an automated desktop pool, View dynamically provisions machines based on settings that you apply to the pool. View uses a virtual machine template as the basis of the pool. From the template, View creates a new virtual machine in vCenter Server for each desktop.

Worksheet for Creating an Automated Pool That Contains Full Virtual Machines

When you create an automated desktop pool, the View Administrator Add Desktop Pool wizard prompts you to configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

You can print this worksheet and write down the values you want to specify when you run the Add Desktop Pool wizard.

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines

Option	Description	Fill In Your Value Here
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a machine. Users receive the same machine each time they log in to the pool. ■ In a floating-assignment pool, users receive different machines each time they log in. For details, see "User Assignment in Desktop Pools," on page 99.	
Enable automatic assignment	In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users. If you do not enable automatic assignment, you must explicitly assign a machine to each user. You can assign machines manually even when automatic assignment is enabled.	
vCenter Server	Select the vCenter Server that manages the virtual machines in the pool.	
Desktop Pool ID	The unique name that identifies the pool in View Administrator. If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID. A View Connection Server configuration can be a standalone View Connection Server instance or a pod of replicated instances that share a common View LDAP configuration.	
Display name	The pool name that users see when they log in from a client device. If you do not specify a display name, the pool ID is displayed to users.	
Access group	Select an access group in which to place the pool or leave the pool in the default root access group. If you use an access group, you can delegate managing the pool to an administrator who has a specific role. For details, see the role-based delegated administration chapter in the *View Administration* document. **NOTE** Access groups are different from vCenter Server folders that store desktop virtual machines. You select a vCenter Server folder later in the wizard with other vCenter Server settings.	
Delete machine after logoff	If you select floating user assignment, choose whether to delete machines after users log off. **NOTE** You set this option on the Desktop Pool Settings page.	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

Option	Description	Fill In Your Value Here
Desktop Pool Settings	Settings that determine the desktop state, power status when a virtual machine is not in use, display protocol, Adobe Flash quality, and so on. For descriptions, see "Desktop Pool Settings for All Desktop Pool Types," on page 107. For a list of the settings that apply to automated pools, see "Desktop Settings for Automated Pools That Contain Full Virtual Machines," on page 57. For more information about power policies and automated pools, see "Setting Power Policies for Desktop Pools," on page 112.	
Stop provisioning on error	You can direct View to stop provisioning or continue to provision virtual machines in a desktop pool after an error occurs during the provisioning of a virtual machine. If you leave this setting selected, you can prevent a provisioning error from recurring on multiple virtual machines.	
Virtual Machine Naming	Choose whether to provision machines by manually specifying a list of machine names or by providing a naming pattern and the total number of machines. For details, see "Naming Machines Manually or Providing a Naming Pattern," on page 100.	
Specify names manually	If you specify names manually, prepare a list of machine names and, optionally, the associated user names.	
Naming Pattern	If you use this naming method, provide the pattern. The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine. For details, see "Using a Naming Pattern for Automated Desktop Pools," on page 102.	
Maximum number of machines	If you use a naming pattern, specify the total number of machines in the pool. You can also specify a minimum number of machines to provision when you first create the pool.	
Number of spare (powered on) machines	If you specify names manually or use a naming pattern, specify a number of machines to keep available and powered on for new users. For details, see "Naming Machines Manually or Providing a Naming Pattern," on page 100. When you specify names manually, this option is called # **Unassigned machines kept powered on**.	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

Option	Description	Fill In Your Value Here
Minimum number of machines	If you use a naming pattern and provision machines on demand, specify a minimum number of machines in the pool. The minimum number of machines is created when you create the pool. If you provision machines on demand, additional machines are created as users connect to the pool for the first time or as you assign machines to users.	
Use vSphere Virtual SAN	Specify whether to use Virtual SAN, if available. Virtual SAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts. For more information, see "Using Virtual SAN for High-Performance Storage and Policy-Based Management," on page 141.	
Template	Select the virtual machine template to use for creating the pool.	
vCenter Server folder	Select the folder in vCenter Server in which the desktop pool resides.	
Host or cluster	Select the ESXi host or cluster on which the virtual machines run. In vSphere 5.1 or later, you can select a cluster with up to 32 ESXi hosts.	
Resource pool	Select the vCenter Server resource pool in which the desktop pool resides.	
Datastores	Select one or more datastores on which to store the desktop pool. For clusters, you can use shared or local datastores. **Note** If you use Virtual SAN, select only one datastore.	
Use View Storage Accelerator	Determine whether ESXi hosts cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is supported on vSphere 5.0 and later. This feature is enabled by default. For details, see "Configure View Storage Accelerator for View Composer Linked Clones," on page 156.	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

Option	Description	Fill In Your Value Here
Transparent Page Sharing Scope	Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Pool**, **Pod**, or **Global**. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you enable TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by Horizon 7 on the same ESXi host can share memory pages, regardless of which pool the machines reside in. **NOTE** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	
Guest customization	Select a customization specification (SYSPREP) from the list to configure licensing, domain attachment, DHCP settings, and other properties on the machines. Alternatively, you can customize the machines manually after they are created.	

Create an Automated Pool That Contains Full Virtual Machines

You can create an automated desktop pool based on a virtual machine template that you select. View dynamically deploys the desktops, creating a new virtual machine in vCenter Server for each desktop.

Prerequisites

- Prepare a virtual machine template that View will use to create the machines. Horizon Agent must be installed on the template. See Chapter 4, "Creating and Preparing a Parent Virtual Machine for Cloning," on page 19.
- If you intend to use a customization specification, make sure that the specifications are accurate. In vSphere Client, deploy and customize a virtual machine from your template using the customization specification. Fully test the resulting virtual machine, including DHCP and authentication.
- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools. The number of virtual switch ports on the ESXi host must equal or exceed the number of virtual machines multiplied by the number of virtual NICs per virtual machine.
- Gather the configuration information you must provide to create the pool. See "Worksheet for Creating an Automated Pool That Contains Full Virtual Machines," on page 51.
- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See "Desktop Pool Settings for All Desktop Pool Types," on page 107.

- If you intend to provide access to your desktops and applications through VMware Identity Manager, verify that you create the desktop and application pools as a user who has the Administrators role on the root access group in View Administrator. If you give the user the Administrators role on an access group other than the root access group, VMware Identity Manager will not recognize the SAML authenticator you configure in View, and you cannot configure the pool in VMware Identity Manager.

Procedure

1. In View Administrator, select **Catalog > Desktop Pools**.
2. Click **Add**.
3. Select **Automated Desktop Pool**.
4. On the vCenter Server page, choose **Full virtual machines**.
5. Follow the prompts in the wizard to create the pool.

   Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

In View Administrator, you can view the machines as they are added to the pool by selecting **Catalog > Desktop Pools**.

What to do next

Entitle users to access the pool. See “Add Entitlements to a Desktop or Application Pool,” on page 131.

Clone an Automated Desktop Pool

You can clone an automated desktop pool from an existing pool. When you clone a pool, the existing desktop pool's settings are copied into the Add Desktop Pool wizard, allowing you to create a new pool without having to fill in each setting manually.

With this feature, you can streamline pool creation because you do not have to type every option in the Add Desktop Pool wizard. You can ensure that desktop pool attributes are standardized by using the pre-filled values in the wizard.

You can clone automated desktop pools that contain full virtual machines or View Composer linked clones. You cannot clone automated desktop pools of instant clones, manual desktop pools, or RDS desktop pools.

When you clone a desktop pool, you cannot change certain settings:

- Desktop pool type
- Clone type, either linked clone or full virtual machine
- User assignment, either dedicated or floating
- vCenter Server instance

Prerequisites

- Verify that the prerequisites for creating the original desktop pool are still valid.

  For example, for a pool that contains full virtual machines, verify that a virtual machine template was prepared.

  For a linked-clone pool, verify that a parent virtual machine was prepared and a snapshot was taken after the virtual machine was powered off.

  When you clone a pool, you can use the same virtual machine template or parent virtual machine, or you can select another one.

- For prerequisites for cloning an automated, full-clone pool, see "Create an Automated Pool That Contains Full Virtual Machines," on page 55.
- For prerequisites for cloning a linked-cone pool, see "Create a Linked-Clone Desktop Pool," on page 69.

Procedure

1 In View Administrator, select **Catalog > Desktop Pools**.

2 Select the desktop pool that you want to clone and click **Clone**.

The Add Desktop Pool wizard appears.

3 On the Add Desktop Pool page, type a unique pool ID.

4 On the Provisioning Settings page, provide unique names for the virtual machines.

Option	Description
Use a naming pattern	Type a virtual machine naming pattern.
Specify names manually	Provide a list of unique names for the virtual machines.

5 Follow the other prompts in the wizard to create the pool.

Change desktop pool settings and values as needed.

In View Administrator, you can view the machines as they are added to the pool by selecting **Catalog > Desktop Pools**.

What to do next

Entitle users to access the pool. See "Add Entitlements to a Desktop or Application Pool," on page 131.

Desktop Settings for Automated Pools That Contain Full Virtual Machines

You must specify desktop pool settings when you configure automated pools that contain full virtual machines. Different settings apply to pools with dedicated user assignments and floating user assignments.

Table 5-2 lists the settings that apply to automated pools with dedicated assignments and floating assignments.

For descriptions of each desktop pool setting, see "Desktop Pool Settings for All Desktop Pool Types," on page 107.

Table 5-2. Settings for Automated Pools That Contain Full Virtual Machines

Setting	Automated Pool, Dedicated Assignment	Automated Pool, Floating Assignment
State	Yes	Yes
Connection Server restrictions	Yes	Yes
Remote machine power policy	Yes	Yes
Automatic logoff after disconnect	Yes	Yes
Allow users to reset/restart their machines	Yes	Yes
Allow user to initiate separate sessions from different client devices		Yes
Delete machine after logoff		Yes

Table 5-2. Settings for Automated Pools That Contain Full Virtual Machines (Continued)

Setting	Automated Pool, Dedicated Assignment	Automated Pool, Floating Assignment
Default display protocol	Yes	Yes
Allow users to choose protocol	Yes	Yes
3D Renderer	Yes	Yes
Max number of monitors	Yes	Yes
Max resolution of any one monitor	Yes	Yes
Adobe Flash quality	Yes	Yes
Adobe Flash throttling	Yes	Yes
Override global Mirage settings	Yes	Yes
Mirage Server configuration	Yes	Yes

Configure Full Clones with vSphere Virtual Machine Encryption

You can configure full clones to use the vSphere Virtual Machine Encryption feature. You can create full-clone desktops that have the same encryption keys or, full-clone desktops with different keys.

Prerequisites

- vSphere 6.5 or later.
- Create the Key Management Server (KMS) cluster with key management servers.
- To create a trust between KMS and vCenter Server, accept the self signed CA certificate or create a CA signed certificate.
- In vSphere Web Client, create the `VMcrypt/VMEncryption` storage profile.
- Horizon 7

Note For details about the Virtual Machine Encryption feature in vSphere, see the *vSphere Security* document in the vSphere documentation.

Procedure

1 To configure full clones that use the same encryption keys, create a parent template for all desktops to have the same encryption keys.

The clone inherits the parent encryption state including keys.

a In vSphere Web Client, create a parent VM with the `vmencrypt` storage policy or create a parent VM and then apply the `vmencrypt` storage policy.

b Convert the parent VM to a virtual machine template.

c Create full-clone desktops that point to the parent template so that all desktops have the same encryption keys.

Note Do not select the Content Based Read Cache (CBRC) feature when you create the full-clone desktop pool. The CBRC and Virtual Machine Encryption features are not compatible.

2 To configure full clones that use different encryption keys, you must change the storage policy for each full-clone desktop.

   a In vSphere Web Client, create the full-clone desktop pool and then edit the full-clone desktops.

      You can also edit existing full-clone desktops.

   b Navigate to each full-clone desktop and edit the storage policy and change the storage policy to `vmencrypt`.

      Each full-clone desktop gets a different encryption key.

Note Full-clone desktops with CBRC digestive disks that exist cannot get the `vmencrypt` storage policy. The `vmencrypt` storage policy applies only when the parent VM does not have any snapshots.

Creating Linked-Clone Desktop Pools 6

With a linked-clone desktop pool, View creates a desktop pool based on a parent virtual machine that you select. The View Composer service dynamically creates a new linked-clone virtual machine in vCenter Server for each desktop.

This chapter includes the following topics:

Linked-Clone Desktop Pools

To create a linked-clone desktop pool, View Composer generates linked-clone virtual machines from a snapshot of a parent virtual machine. View dynamically provisions the linked-clone desktops based on settings that you apply to the pool.

Because linked-clone desktops share a base system-disk image, they use less storage than full virtual machines.

Worksheet for Creating a Linked-Clone Desktop Pool

When you create a linked-clone desktop pool, the View Administrator Add Desktop Pool wizard prompts you to configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

You can print this worksheet and write down the values you want to specify when you run the Add Desktop Pool wizard.

Before you create a linked-clone pool, you must use vCenter Server to take a snapshot of the parent virtual machine that you prepare for the pool. You must shut down the parent virtual machine before you take the snapshot. View Composer uses the snapshot as the base image from which the clones are created.

Note You cannot create a linked-clone pool from a virtual machine template.

Table 6-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool

Option	Description	Fill In Your Value Here
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a machine. Users receive the same machine each time they log in. ■ In a floating-assignment pool, users receive different machines each time they log in. For details, see "User Assignment in Desktop Pools," on page 99.	
Enable automatic assignment	In a dedicated-assignment pool, a machine is assigned to a user when the user first logs in to the pool. You can also explicitly assign machines to users. If you do not enable automatic assignment, you must explicitly assign a machine to each user.	
vCenter Server	Select the vCenter Server that manages the virtual machines in the pool.	
Desktop Pool ID	The unique name that identifies the pool in View Administrator. If multiple View Connection Server configurations are running in your environment, make sure that another View Connection Server configuration is not using the same pool ID. A View Connection Server configuration can be a standalone View Connection Server instance or a pod of replicated instances that share a common View LDAP configuration.	
Display name	The pool name that users see when they log in from a client device. If you do not specify a display name, the pool ID is displayed to users.	
Access group	Select an access group in which to place the pool or leave the pool in the default root access group. If you use an access group, you can delegate managing the pool to an administrator who has a specific role. For details, see the role-based delegated administration chapter in the *View Administration* document. **NOTE** Access groups are different from vCenter Server folders that store virtual machines that are used as desktops. You select a vCenter Server folder later in the wizard with other vCenter Server settings.	
Delete or refresh machine on logoff	If you select floating user assignment, choose whether to refresh machines, delete machines, or do nothing after users log off. **NOTE** You set this option on the Desktop Pool Settings page.	
Desktop Pool Settings	Settings that determine the machine state, power status when a virtual machine is not in use, display protocol, Adobe Flash quality, and so on. For descriptions, see "Desktop Pool Settings for All Desktop Pool Types," on page 107. For a list of the settings that apply to linked-clone pools, see "Desktop Pool Settings for Linked-Clone Desktop Pools," on page 72. For more information about power policies and automated pools, see "Setting Power Policies for Desktop Pools," on page 112.	

Table 6-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Stop provisioning on error	You can direct View to stop provisioning or continue to provision virtual machines in a desktop pool after an error occurs during the provisioning of a virtual machine. If you leave this setting selected, you can prevent a provisioning error from recurring on multiple virtual machines.	
Virtual machine naming	Choose whether to provision machines by manually specifying a list of machine names or by providing a naming pattern and the total number of machines. For details, see "Naming Machines Manually or Providing a Naming Pattern," on page 100.	
Specify names manually	If you specify names manually, prepare a list of machine names and, optionally, the associated user names.	
Naming pattern	If you use this naming method, provide the pattern. The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine. For details, see "Using a Naming Pattern for Automated Desktop Pools," on page 102.	
Max number of machines	If you use a naming pattern, specify the total number of machines in the pool. You can also specify a minimum number of machines to provision when you first create the pool.	
Number of spare (powered on) machines	If you specify names manually or use a naming pattern, specify a number of machines to keep available and powered on for new users. For details, see "Naming Machines Manually or Providing a Naming Pattern," on page 100. When you specify names manually, this option is called # **Unassigned machines kept powered on**.	
Minimum number of ready (provisioned) machines during View Composer maintenance operations	If you specify names manually or use a naming pattern, specify a minimum number of machines that are provisioned for use in remote desktop sessions while View Composer maintenance operations take place. This setting allows users to maintain existing connections or make new connection requests while View Composer refreshes, recomposes, or rebalances the machines in the pool. The setting does not distinguish between spare machines that are ready to accept new connections and machines that are already connected in existing desktop sessions. This value must be smaller than the **Max number of machines**, which you specify if you provision machines on demand. See "Keeping Linked-Clone Machines Provisioned for Use in Remote Desktop Sessions During View Composer Operations," on page 77.	

Table 6-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Provision machines on demand or Provision all machines up front	If you use a naming pattern, choose whether to provision all machines when the pool is created or provision machines as they are needed. - **Provision all machines up front**. When the pool is created, the system provisions the number of machines you specify in **Max number of machines**. - **Provision machines on demand**. When the pool is created, the system creates the number of machines that you specify in **Min number of machines**. Additional machines are created as users connect to the pool for the first time or as you assign machines to users.	
Min number of machines	If you use a naming pattern and provision desktops on demand, specify a minimum number of machines in the pool. The system creates the minimum number of machines when you create the pool. This number is maintained even when other settings such as **Delete or refresh machine on logoff** cause machines to be deleted.	
Redirect Windows profile to a persistent disk	If you select dedicated user assignments, choose whether to store Windows user-profile data on a separate View Composer persistent disk or the same disk as the OS data. Separate persistent disks let you preserve user data and settings. View Composer refresh, recompose, and rebalance operations do not affect persistent disks. You can detach a persistent disk from a linked clone and recreate the linked-clone virtual machine from the detached disk. For example, when a machine or pool is deleted, you can detach the persistent disk and recreate the desktop, preserving the original user data and settings. If you store the Windows profile in the OS disk, user data and settings are removed during refresh, recompose, and rebalance operations.	
Disk size and drive letter for persistent disk	If you store user profile data on a separate View Composer persistent disk, provide the disk size in megabytes and the drive letter. **NOTE** Do not select a drive letter that already exists on the parent virtual machine or that conflicts with a drive letter that is used for a network-mounted drive.	
Disposable File Redirection	Choose whether to redirect the guest OS's paging and temp files to a separate, nonpersistent disk. If you do, provide the disk size in megabytes. With this configuration, when a linked clone is powered off, the disposable-file disk is replaced with a copy of the original disk that was created with the linked-clone pool. Linked clones can increase in size as users interact with their desktops. Disposable file redirection can save storage space by slowing the growth of linked clones.	

Table 6-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Disk size and drive letter for disposable file disk	If you redirect disposable files to a nonpersistent disk, provide the disk size in megabytes and the drive letter. The disk size should be larger than page-file size of the guest OS. To determine the page-file size, see "Record the Paging File Size of a View Composer Parent Virtual Machine," on page 48. When you configure the disposable file disk size, consider that the actual size of a formatted disk partition is slightly smaller than the value you provide in View Administrator. You can select a drive letter for the disposable file disk. The default value, **Auto**, directs View to assign the drive letter. **Note** Do not select a drive letter that already exists on the parent virtual machine or that conflicts with a drive letter that is used for a network-mounted drive.	
Use vSphere Virtual SAN	Specify whether to use VMware Virtual SAN, if available. Virtual SAN is a software-defined storage tier that virtualizes the local physical storage disks available on a cluster of ESXi hosts. For more information, see "Using Virtual SAN for High-Performance Storage and Policy-Based Management," on page 141.	
Select separate datastores for persistent and OS disks	(Available only if you do not use Virtual SAN) If you redirect user profiles to separate persistent disks, you can store the persistent disks and OS disks on different datastores.	
Select separate datastores for replica and OS disks	(Available only if you do not use Virtual SAN or Virtual Volumes) You can store the replica (master) virtual machine disk on a high performance datastore and the linked clones on separate datastores. For details, see "Storing Replicas and Clones on Separate Datastores for Instant Clones and View Composer Linked Clones," on page 155. If you store replicas and OS disks on separate datastores, native NFS snapshots cannot be used. Native cloning on a NAS device can only take place if the replica and OS disks are stored on the same datastores.	
Parent VM	Select the parent virtual machine for the pool.	
Snapshot (default image)	Select the snapshot of the parent virtual machine to use as the base image for the pool. Do not delete the snapshot and parent virtual machine from vCenter Server, unless no linked clones in the pool use the default image, and no more linked clones will be created from this default image. The system requires the parent virtual machine and snapshot to provision new linked clones in the pool, according to pool policies. The parent virtual machine and snapshot are also required for View Composer maintenance operations.	
VM folder location	Select the folder in vCenter Server in which the desktop pool resides.	

Table 6-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Host or cluster	Select the ESXi host or cluster on which the desktop virtual machines run. With Virtual SAN datastores (a vSphere 5.5 Update 1 feature), you can select a cluster with up to 20 ESXi hosts. With Virtual Volumes datastores (a vSphere 6.0 feature), you can select a cluster with up to 32 ESXi hosts. In vSphere 5.1 or later, you can select a cluster with up to 32 ESXi hosts if the replicas are stored on VMFS5 or later datastores or NFS datastores. If you store replicas on a VMFS version earlier than VMFS5, a cluster can have at most eight hosts. In vSphere 5.0, you can select a cluster with more than eight ESXi hosts if the replicas are stored on NFS datastores. If you store replicas on VMFS datastores, a cluster can have at most eight hosts. See "Configuring Desktop Pools on Clusters With More Than Eight Hosts," on page 129.	
Resource pool	Select the vCenter Server resource pool in which the desktop pool resides.	
Datastores	Select one or more datastores on which to store the desktop pool. A table on the Select Linked Clone Datastores page of the Add Desktop Pool wizard provides high-level guidelines for estimating the pool's storage requirements. These guidelines can help you determine which datastores are large enough to store the linked-clone disks. For details, see "Storage Sizing for Instant-Clone and View Composer Linked-Clone Desktop Pools," on page 147. You can use shared or local datastores for an individual ESXi host or for ESXi clusters. If you use local datastores in an ESXi cluster, you must consider the vSphere infrastructure constraints that are imposed on your desktop deployment. See "Storing View Composer Linked Clones on Local Datastores," on page 154. With Virtual SAN datastores (a vSphere 5.5 Update 1 feature), you can select a cluster with up to 20 ESXi hosts. With Virtual Volumes datastores (a vSphere 6.0 feature), you can select a cluster with up to 32 ESXi hosts. In vSphere 5.1 or later, a cluster can have more than eight ESXi hosts if the replicas are stored on datastores that are VMFS5 or later or NFS. In vSphere 5.0, a cluster can have more than eight ESXi hosts only if the replicas are stored on NFS datastores. See "Configuring Desktop Pools on Clusters With More Than Eight Hosts," on page 129. For more information about the disks that are created for linked clones, see "View Composer Linked-Clone Data Disks," on page 153. **Note** If you use Virtual SAN, select only one datastore.	

Table 6-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Storage Overcommit	Determine the storage-overcommit level at which linked-clones are created on each datastore. As the level increases, more linked clones fit on the datastore and less space is reserved to let individual clones grow. A high storage-overcommit level lets you create linked clones that have a total logical size larger than the physical storage limit of the datastore. For details, see "Set the Storage Overcommit Level for Linked-Clone Virtual Machines," on page 152. **NOTE** This setting has no effect if you use Virtual SAN.	
Use View Storage Accelerator	Determine whether to use View Storage Accelerator, which allows ESXi hosts to cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is supported on vSphere 5.0 and later. This feature is enabled by default. For details, see "Configure View Storage Accelerator for View Composer Linked Clones," on page 156.	
Use native NFS snapshots (VAAI)	(Available only if you do not use Virtual SAN) If your deployment includes NAS devices that support the vStorage APIs for Array Integration (VAAI), you can use native snapshot technology to clone virtual machines. You can use this feature only if you select datastores that reside on NAS devices that support native cloning operations through VAAI. You cannot use this feature if you store replicas and OS disks on separate datastores. You cannot use this feature on virtual machines with space-efficient disks. This feature is supported on vSphere 5.0 and later. For details, see "Using VAAI Storage for View Composer Linked Clones," on page 159.	
Reclaim VM disk space	(Available only if you do not use Virtual SAN or Virtual Volumes) Determine whether to allow ESXi hosts to reclaim unused disk space on linked clones that are created in space-efficient disk format. The space reclamation feature reduces the total storage space required for linked-clone desktops. This feature is supported on vSphere 5.1 and later. The linked-clone virtual machines must be virtual hardware version 9 or later. For details, see "Reclaim Disk Space on View Composer Linked Clones," on page 157.	

Table 6-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Initiate reclamation when unused space on VM exceeds:	(Available only if you do not use Virtual SAN or Virtual Volumes) Type the minimum amount of unused disk space, in gigabytes, that must accumulate on a linked-clone OS disk to trigger space reclamation. When the unused disk space exceeds this threshold, View initiates the operation that directs the ESXi host to reclaim space on the OS disk. This value is measured per virtual machine. The unused disk space must exceed the specified threshold on an individual virtual machine before View starts the space reclamation process on that machine. For example: **2** GB. The default value is 1 GB.	
Blackout Times	Configure days and times during which View Storage Accelerator regeneration and the reclamation of virtual machine disk space do not take place. To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days. For details, see "Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones," on page 160.	
Transparent Page Sharing Scope	Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Pool**, **Pod**, or **Global**. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you enable TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by Horizon 7 on the same ESXi host can share memory pages, regardless of which pool the machines reside in. **Note** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	
Domain	Select the Active Directory domain and user name. View Composer requires certain user privileges to create a linked-clone pool. The domain and user account are used by QuickPrep or Sysprep to customize the linked-clone machines. You specify this user when you configure View Composer settings for vCenter Server. You can specify multiple domains and users when you configure View Composer settings. When you use the Add Desktop Pool wizard to create a pool, you must select one domain and user from the list. For information about configuring View Composer, see the *View Administration* document.	

Table 6-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
AD container	Provide the Active Directory container relative distinguished name. For example: **`CN=Computers`** When you run the Add Desktop Pool wizard, you can browse your Active Directory tree for the container.	
Allow reuse of pre-existing computer accounts	Select this option to use existing computer accounts in Active Directory for linked clones that are provisioned by View Composer. This option lets you control the computer accounts that are created in Active Directory. When a linked clone is provisioned, if an existing AD computer account name matches the linked clone machine name, View Composer uses the existing computer account. Otherwise, a new computer account is created. The existing computer accounts must be located in the Active Directory container that you specify with the **Active Directory container** setting. When this option is disabled, a new AD computer account is created when View Composer provisions a linked clone. This option is disabled by default. For details, see "Use Existing Active Directory Computer Accounts for Linked Clones," on page 78.	
Use QuickPrep or a customization specification (Sysprep)	Choose whether to use QuickPrep or select a customization specification (Sysprep) to configure licensing, domain attachment, DHCP settings, and other properties on the machines. Sysprep is supported for linked clones only on vSphere 4.1 or later software. After you use QuickPrep or Sysprep when you create a pool, you cannot switch to the other customization method later on, when you create or recompose machines in the pool. For details, see "Choosing QuickPrep or Sysprep to Customize Linked-Clone Machines," on page 74.	
Power-off script	QuickPrep can run a customization script on linked-clone machines before they are powered off. Provide the path to the script on the parent virtual machine and the script parameters.	
Post-synchronization script	QuickPrep can run a customization script on linked-clone machines after they are created, recomposed, and refreshed. Provide the path to the script on the parent virtual machine and the script parameters.	

Create a Linked-Clone Desktop Pool

You can create an automated, linked-clone desktop pool based on a parent virtual machine that you select. The View Composer service dynamically creates a new linked-clone virtual machine in vCenter Server for each desktop.

To create an automated pool that contains full virtual machines, see "Automated Pools That Contain Full Virtual Machines," on page 51.

Prerequisites

- Verify that the View Composer service is installed, either on the same host as vCenter Server or on a separate host, and that a View Composer database is configured. See the *View Installation* document.
- Verify that View Composer settings for vCenter Server are configured in View Administrator. See the *View Administration* document.
- Verify that you have a sufficient number of ports on the ESXi virtual switch that is used for the virtual machines that are used as remote desktops. The default value might not be sufficient if you create large desktop pools. The number of virtual switch ports on the ESXi host must equal or exceed the number of virtual machines multiplied by the number of virtual NICs per virtual machine.
- Verify that you prepared a parent virtual machine. Horizon Agent must be installed on the parent virtual machine. See Chapter 4, "Creating and Preparing a Parent Virtual Machine for Cloning," on page 19.
- Take a snapshot of the parent virtual machine in vCenter Server. You must shut down the parent virtual machine before you take the snapshot. View Composer uses the snapshot as the base image from which the clones are created.

  Note You cannot create a linked-clone pool from a virtual machine template.
- Gather the configuration information you must provide to create the pool. See "Worksheet for Creating a Linked-Clone Desktop Pool," on page 61.
- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See "Desktop Pool Settings for All Desktop Pool Types," on page 107.
- If you intend to provide access to your desktops and applications through VMware Identity Manager, verify that you create the desktop and application pools as a user who has the Administrators role on the root access group in View Administrator. If you give the user the Administrators role on an access group other than the root access group, VMware Identity Manager will not recognize the SAML authenticator you configure in View, and you cannot configure the pool in VMware Identity Manager.

Important While a linked-clone pool is created, do not modify the parent virtual machine in vCenter Server. For example, do not convert the parent virtual machine to a template. The View Composer service requires that the parent virtual machine remain in a static, unaltered state during pool creation.

Procedure

1 In View Administrator, select **Catalog > Desktop Pools**.

2 Click **Add**.

3 Select **Automated Desktop Pool**.

4 On the vCenter Server page, choose **View Composer linked clones**.

5 Follow the prompts in the wizard to create the pool.

  Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page you completed by clicking the page name in the navigation panel.

  On the **vCenter Settings** page, you must click **Browse** and select the vCenter Server settings in sequence. You cannot skip a vCenter Server setting:

  a Parent VM

  b Snapshot

  c VM folder location

  d Host or cluster

e Resource pool

f Datastores

In View Administrator, you can view the machines as they are added to the pool by selecting **Catalog > Desktop Pools**.

The linked clones might restart one or more times while they are provisioned. If a linked clone is in an error state, the View automatic recovery mechanism attempts to power on, or shut down and restart, the linked clone. If repeated recovery attempts fail, the linked clone is deleted.

View Composer also creates a replica virtual machine that serves as the master image for provisioning the linked clones. To reduce space consumption, the replica is created as a thin disk. If all the virtual machines are recomposed or deleted, and no clones are linked to the replica, the replica virtual machine is deleted from vCenter Server.

If you do not store the replica on a separate datastore, View Composer creates a replica on each datastore on which linked clones are created.

If you store the replica on a separate datastore, one replica is created for the entire pool, even when linked clones are created on multiple datastores.

What to do next

Entitle users to access the pool. See "Add Entitlements to a Desktop or Application Pool," on page 131.

Clone an Automated Desktop Pool

You can clone an automated desktop pool from an existing pool. When you clone a pool, the existing desktop pool's settings are copied into the Add Desktop Pool wizard, allowing you to create a new pool without having to fill in each setting manually.

With this feature, you can streamline pool creation because you do not have to type every option in the Add Desktop Pool wizard. You can ensure that desktop pool attributes are standardized by using the pre-filled values in the wizard.

You can clone automated desktop pools that contain full virtual machines or View Composer linked clones. You cannot clone automated desktop pools of instant clones, manual desktop pools, or RDS desktop pools.

When you clone a desktop pool, you cannot change certain settings:

- Desktop pool type
- Clone type, either linked clone or full virtual machine
- User assignment, either dedicated or floating
- vCenter Server instance

Prerequisites

- Verify that the prerequisites for creating the original desktop pool are still valid.

  For example, for a pool that contains full virtual machines, verify that a virtual machine template was prepared.

  For a linked-clone pool, verify that a parent virtual machine was prepared and a snapshot was taken after the virtual machine was powered off.

  When you clone a pool, you can use the same virtual machine template or parent virtual machine, or you can select another one.

- For prerequisites for cloning an automated, full-clone pool, see "Create an Automated Pool That Contains Full Virtual Machines," on page 55.

- For prerequisites for cloning a linked-cone pool, see "Create a Linked-Clone Desktop Pool," on page 69.

Procedure

1 In View Administrator, select **Catalog > Desktop Pools**.

2 Select the desktop pool that you want to clone and click **Clone**.

The Add Desktop Pool wizard appears.

3 On the Add Desktop Pool page, type a unique pool ID.

4 On the Provisioning Settings page, provide unique names for the virtual machines.

Option	Description
Use a naming pattern	Type a virtual machine naming pattern.
Specify names manually	Provide a list of unique names for the virtual machines.

5 Follow the other prompts in the wizard to create the pool.

Change desktop pool settings and values as needed.

In View Administrator, you can view the machines as they are added to the pool by selecting **Catalog > Desktop Pools**.

What to do next

Entitle users to access the pool. See "Add Entitlements to a Desktop or Application Pool," on page 131.

Desktop Pool Settings for Linked-Clone Desktop Pools

You must specify machine and desktop pool settings when you configure automated pools that contain linked clones created by View Composer. Different settings apply to pools with dedicated user assignments and floating user assignments.

Table 6-2 lists the settings that apply to linked-clone pools with dedicated assignments and floating assignments.

For descriptions of each setting, see "Desktop Pool Settings for All Desktop Pool Types," on page 107.

Table 6-2. Settings for Automated, Linked-Clone Desktop Pools

Setting	Linked-Clone Pool, Dedicated Assignment	Linked-Clone Pool, Floating Assignment
State	Yes	Yes
Connection Server restrictions	Yes	Yes
Remote machine power policy	Yes	Yes
Automatically logoff after disconnect	Yes	Yes
Allow users to reset/restart their machines	Yes	Yes
Allow user to initiate separate sessions from different client devices		Yes
Delete or refresh machine on logoff		Yes
Refresh OS disk after logoff	Yes	
Default display protocol	Yes	Yes
Allow users to choose protocol	Yes	Yes
3D Renderer	Yes	Yes

Table 6-2. Settings for Automated, Linked-Clone Desktop Pools (Continued)

Setting	Linked-Clone Pool, Dedicated Assignment	Linked-Clone Pool, Floating Assignment
Max number of monitors	Yes	Yes
Max resolution of any one monitor	Yes	Yes
Adobe Flash quality	Yes	Yes
Adobe Flash throttling	Yes	Yes
Override global Mirage settings	Yes	Yes
Mirage Server configuration	Yes	Yes

View Composer Support for Linked-Clone SIDs and Third-Party Applications

View Composer can generate and preserve local computer security identifiers (SIDs) for linked-clone virtual machines in some situations. View Composer can preserve globally unique identifiers (GUIDs) of third-party applications, depending on the way that the applications generate GUIDs.

To understand how View Composer operations affect SIDs and application GUIDs, you should understand how linked-clone machines are created and provisioned:

1. View Composer creates a linked clone by taking these actions:

   a. Creates the replica by cloning the parent virtual-machine snapshot.

   b. Creates the linked clone to refer to the replica as its parent disk.

2. View Composer and View customize the linked clone with QuickPrep or a Sysprep customization specification, depending on which customization tool you select when you create the pool.

   - If you use Sysprep, a unique SID is generated for each clone.
   - If you use QuickPrep, no new SID is generated. The parent virtual machine's SID is replicated on all provisioned linked-clone machines in the pool.
   - Some applications generate a GUID during customization.

3. View creates a snapshot of the linked clone.

   The snapshot contains the unique SID generated with Sysprep or common SID generated with QuickPrep.

4. View powers on the machine according to the settings you select when you create the pool.

   Some applications generate a GUID the first time the machine is powered on.

For a comparison of QuickPrep and Sysprep customization, see "Choosing QuickPrep or Sysprep to Customize Linked-Clone Machines," on page 74.

When you refresh the linked clone, View Composer uses the snapshot to restore the clone to its initial state. Its SID is preserved.

If you use QuickPrep, when you recompose the linked clone, the parent virtual machine's SID is preserved on the linked clone as long as you select the same parent virtual machine for the recompose operation. If you select a different parent virtual machine for the recomposition, the new parent's SID is replicated on the clone.

If you use Sysprep, a new SID is always generated on the clone. For details, see "Recomposing Linked Clones Customized with Sysprep," on page 77.

Table 6-3 shows the effect of View Composer operations on linked-clone SIDs and third-party application GUIDs.

Table 6-3. View Composer Operations, Linked-Clone SIDs, and Application GUIDs

Support for SIDs or GUIDs	Clone Creation	Refresh	Recompose
Sysprep: Unique SIDs for linked clones	With Sysprep customization, unique SIDs are generated for linked clones.	Unique SIDs are preserved.	Unique SIDS are not preserved.
QuickPrep: Common SIDs for linked clones	With QuickPrep customization, a common SID is generated for all clones in a pool.	Common SID is preserved.	Common SID is preserved.
Third-party application GUIDs	Each application behaves differently. **NOTE** Sysprep and QuickPrep have the same effect on GUID preservation.	The GUID is preserved if an application generates the GUID before the initial snapshot is taken. The GUID is not preserved if an application generates the GUID after the initial snapshot is taken.	Recompose operations do not preserve an application GUID unless the application writes the GUID on the drive specified as a View Composer persistent disk.

Choosing QuickPrep or Sysprep to Customize Linked-Clone Machines

QuickPrep and Microsoft Sysprep provide different approaches to customizing linked-clone machines. QuickPrep is designed to work efficiently with View Composer. Microsoft Sysprep offers standard customization tools.

When you create linked-clone machines, you must modify each virtual machine so that it can function as a unique computer on the network. View and View Composer provide two methods for personalizing linked-clone machines.

Table 6-4 compares QuickPrep with customization specifications that are created with Microsoft Sysprep.

Table 6-4. Comparing QuickPrep and Microsoft Sysprep

QuickPrep	Customization Specification (Sysprep)
Designed to work with View Composer. For details, see "Customizing Linked-Clone Machines with QuickPrep," on page 75.	Can be created with the standard Microsoft Sysprep tools.
Uses the same local computer security identifier (SID) for all linked clones in the pool.	Generates a unique local computer SID for each linked clone in the pool.
Can run additional customization scripts before linked clones are powered off and after linked clones are created, refreshed, or recomposed.	Can run an additional script when the user first logs in.
Joins the linked clone computer to the Active Directory domain.	Joins the linked-clone computer to the Active Directory domain. The domain and administrator information in the Sysprep customization specification is not used. The virtual machine is joined to the domain using the guest customization information that you enter in View Administrator when you create the pool.
For each linked clone, adds a unique ID to the Active Directory domain account.	For each linked clone, adds a unique ID to the Active Directory domain account.
Does not generate a new SID after linked clones are refreshed. The common SID is preserved.	Generates a new SID when each linked clone is customized. Preserves the unique SIDs during a refresh operation, but not during a recompose or rebalance operation.

Table 6-4. Comparing QuickPrep and Microsoft Sysprep (Continued)

QuickPrep	Customization Specification (Sysprep)
Does not generate a new SID after linked clones are recomposed. The common SID is preserved.	Runs again after linked clones are recomposed, generating new SIDs for the virtual machines. For details, see "Recomposing Linked Clones Customized with Sysprep," on page 77.
Runs faster than Sysprep.	Can take longer than QuickPrep.

After you customize a linked-clone pool with QuickPrep or Sysprep, you cannot switch to the other customization method when you create or recompose machines in the pool.

Customizing Linked-Clone Machines with QuickPrep

You can personalize the linked-clone machines that are created from a parent virtual machine by using the QuickPrep system tool. View Composer executes QuickPrep when a linked-clone machine is created or recomposed.

QuickPrep customizes a linked-clone machine in several ways:

- Gives the computer a name that you specify when you create the linked-clone pool.
- Creates a computer account in Active Directory, joining the computer to the appropriate domain.
- Mounts the View Composer persistent disk. The Windows user profile is redirected to this disk.
- Redirects temp and paging files to a separate disk.

These steps might require the linked clones to restart one or more times.

QuickPrep uses KMS volume license keys to activate Windows linked-clone machines. For details, see the *View Administration* document.

You can create your own scripts to further customize the linked clones. QuickPrep can run two types of scripts at predefined times:

- After linked clones are created or recomposed
- Immediately before linked clones are powered off

For guidelines and rules for using QuickPrep customization scripts, see "Running QuickPrep Customization Scripts," on page 75.

Note View Composer requires domain user credentials to join linked-clone machines to an Active Directory domain. For details, see the *View Administration* document.

Running QuickPrep Customization Scripts

With the QuickPrep tool, you can create scripts to customize the linked-clone machines in a pool. You can configure QuickPrep to run customization scripts at two predefined times.

When QuickPrep Scripts Run

The post-synchronization script runs after linked clones are created, recomposed, or rebalanced, and the clones' status is **Ready**. The power-off script runs before linked clones are powered off. The scripts run in the guest operating systems of the linked clones.

How QuickPrep Executes Scripts

The QuickPrep process uses the Windows `CreateProcess` API call to execute scripts. Your script can invoke any process that can be created with the `CreateProcess` API. For example, `cmd`, `vbscript`, `exe`, and batch-file processes work with the API.

In particular, QuickPrep passes the path that is specified for the script as the second parameter to the `CreateProcess` API and sets the first parameter to `NULL`.

For example, if the script path is `c:\myscript.cmd`, the path appears as the second parameter in the function in the View Composer log file: `CreateProcess(NULL,c:\myscript.cmd,...)`.

Providing Paths to QuickPrep Scripts

You provide paths to the QuickPrep customization scripts when you create a linked-clone machine pool or when you edit a pool's guest customization settings. The scripts must reside on the parent virtual machine. You cannot use a UNC path to a network share.

If you use a scripting language that needs an interpreter to execute the script, the script path must start with the interpreter binary.

For example, if you specify the path `C:\script\myvb.vbs` as a QuickPrep customization script, View Composer Agent cannot execute the script. You must specify a path that starts with the interpreter binary path:

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

Important Protect QuickPrep customization scripts from access by ordinary users. Place the scripts in a secure folder.

QuickPrep Script Timeout Limit

View Composer terminates a post-synchronization or power-off script that takes longer than 20 seconds. If your script takes longer than 20 seconds, you can increase the timeout limit. For details, see "Increase the Timeout Limit for ClonePrep and QuickPrep Customization Scripts," on page 49.

Alternatively, you can use your script to launch another script or process that performs the long-running task.

QuickPrep Script Account

QuickPrep runs the scripts under the account under which the VMware View Composer Guest Agent Server service is configured to run. By default, this account is `Local System`.

Do not change this log on account. If you do, the linked clones do not start.

QuickPrep Process Privileges

For security reasons, certain Windows operating system privileges are removed from the View Composer Guest Agent process that invokes QuickPrep customization scripts.

A QuickPrep customization script cannot perform any action that requires a privilege that is removed from the View Composer Guest Agent process.

The following privileges are removed from the process that invokes QuickPrep scripts:

```
SeCreateTokenPrivilege
SeTakeOwnershipPrivilege
SeSecurityPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeSystemtimePrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeLockMemoryPrivilege
```

```
SeIncreaseBasePriorityPrivilege
SeCreatePermanentPrivilege
SeDebugPrivilege
SeAuditPrivilege
```

QuickPrep Script Logs

View Composer logs contain information about QuickPrep script execution. The log records the start and end of execution and logs output or error messages. The log is located in the Windows `temp` directory:

```
C:\Windows\Temp\vmware-viewcomposer-ga-new.log
```

Recomposing Linked Clones Customized with Sysprep

If you recompose a linked-clone machine that was customized with Sysprep, View runs the Sysprep customization specification again after the OS disk is recomposed. This operation generates a new SID for the linked-clone virtual machine.

If a new SID is generated, the recomposed linked clone functions as a new computer on the network. Some software programs such as system-management tools depend on the SID to identify the computers under their management. These programs might not be able to identify or locate the linked-clone virtual machine.

Also, if third-party software is installed on the system disk, the customization specification might regenerate the GUIDs for that software after the recomposition.

A recomposition restores the linked clone to its original state, before the customization specification was run the first time. In this state, the linked clone does not have a local computer SID or the GUID of any third-party software installed in the system drive. View must run the Sysprep customization specification after the linked clone is recomposed.

Keeping Linked-Clone Machines Provisioned for Use in Remote Desktop Sessions During View Composer Operations

If your users must be able to access remote desktops at all times, you must maintain a certain number of machines that are provisioned for use in remote desktop sessions even when View Composer maintenance operations take place. You can set a minimum number of machines that are not placed in maintenance mode while View Composer refreshes, recomposes, or rebalances the linked-clone virtual machines in a pool.

When you set a **Minimum number of ready (provisioned) machines during View Composer maintenance operations**, View ensures that the specified number of machines stay provisioned, and are not placed in maintenance mode, while View Composer proceeds through the maintenance operation.

This setting lets users maintain existing connections or make new connection requests during the View Composer maintenance operation. The setting does not distinguish between spare machines that are ready to accept new connections and machines that are already connected in existing desktop sessions.

You can specify this setting when you create or edit a linked-clone pool.

The following guidelines apply to this setting:

- To allow a number of users to maintain their existing desktop connections and keep a minimum number of spare (powered on) machines that can accept new connection requests, set the **Minimum number of ready (provisioned) machines during View Composer maintenance operations** to a large enough value to include both sets of machines.
- If you use a naming pattern to provision machines and provision machines on demand, set the number of provisioned machines during View Composer operations to a smaller value than the specified **Max number of machines**. If the maximum number were smaller, your pool could end up with fewer total machines than the minimum number you want to keep provisioned during View Composer operations. In this case, View Composer maintenance operations could not take place.

- If you provision machines by manually specifying a list of machine names, do not reduce the total pool size (by removing machine names) to a lower number than the minimum number of provisioned machines. In this case, View Composer maintenance operations could not take place.
- If you set a large minimum number of provisioned machines in relation to the pool size, View Composer maintenance operations might take longer to complete. While View maintains the minimum number of provisioned machines during a maintenance operation, the operation might not reach the concurrency limit that is specified in the **Max concurrent View Composer maintenance operations** setting.

  For example, if a pool contains 20 machines and the minimum number of provisioned machines is 15, View Composer can operate on at most five machines at a time. If the concurrency limit for View Composer maintenance operations is 12, the concurrency limit is never reached.
- In this setting name, the term "ready" applies to the state of the linked-clone virtual machine, not the machine status that is displayed in View Administrator. A virtual machine is ready when it is provisioned and ready to be powered on. The machine status reflects the View-managed condition of the machine. For example, a machine can have a status of `Connected`, `Disconnected`, `Agent Unreachable`, `Deleting`, and so on, and still be considered "ready".

Use Existing Active Directory Computer Accounts for Linked Clones

When you create or edit a desktop pool or an automated farm, you can configure View Composer to use existing computer accounts in Active Directory for newly provisioned linked clones.

By default, View Composer generates a new Active Directory computer account for each linked clone that it provisions. The **Allow reuse of pre-existing computer accounts** option lets you control the computer accounts that are created in Active Directory by ensuring that View Composer uses existing AD computer accounts.

With this option enabled, when a linked clone is provisioned, View Composer checks if an existing AD computer account name matches the linked clone machine name. If a match exists, View Composer uses the existing AD computer account. If View Composer does not find a matching AD computer account name, View Composer generates a new AD computer account for the linked clone.

You can set the **Allow reuse of pre-existing computer accounts** option when you create or edit a desktop pool or an automated farm. If you edit a pool or a farm and set this option, the setting affects linked-clone machines that are provisioned in the future. Linked clones that are already provisioned are not affected.

When you set the **Allow reuse of pre-existing computer accounts** option, you can limit the Active Directory permissions assigned to the View Composer user account that generates the desktop pool or farm. Only the following Active Directory permissions are required:

- List Contents
- Read All Properties
- Read Permissions
- Reset Password

You can only limit the Active Directory permissions if you are sure that all machines you intend to provision have existing computer accounts allocated in Active Directory. View Composer generates a new AD computer account if no matching name is found. Additional permissions such as Create Computer Objects are required to create new computer accounts. For a complete list of permissions required for the View Composer user account, see the *View Administration* document.

This option cannot be disabled if View Composer is currently using at least one existing AD computer account.

The following procedure applies to linked-clone desktop pools. The steps are similar for automated farms.

Prerequisites

Verify that the existing computer accounts are located in the Active Directory container that you specify with the **Active Directory container** setting. If the existing accounts are located in a different container, provisioning fails for linked clones with those account names, and an error message states that the existing computer accounts already exist in Active Directory.

For example, if you select the **Allow reuse of pre-existing computer accounts** option and specify that the **Active Directory container** is the default value, **`CN=Computers`**, and the existing computer accounts are located in **`OU=mydesktops`**, provisioning fails for those accounts.

Procedure

1 In Active Directory, create the computer accounts to use for the linked-clone machines.

   For example: `machine1, machine2, machine3`

   The computer account names must use consecutive integers so that they match the names that are generated during machine provisioning in View.

2 In View Administrator, create a pool by using the Add Desktop Pool wizard or edit the pool in the Edit dialog box.

3 On the Provisioning Settings page or tab, select **Use a naming pattern**.

4 In the **Naming Pattern** text box, type a machine name that matches the Active Directory computer account name.

   For example: `machine`

   View appends unique numbers to the pattern to provide a unique name for each machine.

   For example: `machine1, machine2, machine3`

5 On the Guest Customization page or tab, select the **Allow reuse of pre-existing computer accounts** option.

Creating Instant-Clone Desktop Pools 7

To provide users access to instant-clone desktops, you must create an instant-clone desktop pool.

This chapter includes the following topics:

Instant-Clone Desktop Pools

An instant-clone desktop pool is an automated desktop pool. vCenter Server creates the desktop VMs based on the settings that you specify when you create the pool.

Similar to View Composer linked clones, instant clones share a virtual disk of a parent VM and therefore consume less storage than full VMs. In addition, instant clones share the memory of a parent VM. Instant clones are created using the vmFork technology. An instant-clone desktop pool has the following key characteristics:

- The provisioning of instant clones is significantly faster than View Composer linked clones.
- Instant clones are always created in a powered-on state, ready for users to connect to. Guest customization and joining the Active Directory domain are completed as part of the initial power-on workflow.
- When a user logs out, the desktop VM is deleted. New clones are created according to the provisioning policy, which can be on-demand or up-front.
- With the push-image operation, you can re-create the pool from any snapshot of any parent VM. You can use a push image to roll out operating system and application patches.
- When clones are created, View selects a datastore to achieve the best distribution of the clones across the datastores. No manual rebalancing is necessary.
- View storage accelerator is automatically enabled.
- Transparent page sharing is automatically enabled.

- Instant clones require static port binding.
- Instant clones that use multiple vLAN networks require static port binding with fixed port allocation.

Because View can create instant clones quickly, you do not need to provision desktops up front or have many ready desktops. Compared with View Composer linked clones, instant clones can make the task of managing large desktop pools easier and also reduce the amount of hardware resources that is required.

Instant clones have the following compatibility requirements:

- vSphere 6.0 Update 1 or later.
- Virtual machine hardware version 11 or later.

As a best practice, configure distributed virtual switches in the vSphere environment.

In Horizon 7.0, instant clones have the following restrictions:

- Only single-user desktops are supported. RDS hosts are not supported.
- Only floating user assignment is supported. Users are assigned random desktops from the pool.
- Instant-clone desktops cannot have persistent disks. Users can use VMware App Volumes to store persistent data. For more information about App Volumes, see https://www.vmware.com/products/appvolumes.
- Virtual Volumes and VAAI (vStorage APIs for Array Integration) native NFS snapshots are not supported.
- Sysprep is not available for desktop customization.
- Windows 7 and Windows 10 are supported but not Windows 8 or Windows 8.1.
- PowerCLI is not supported.
- Local datastores are not supported.
- IPv6 is not supported.
- Instant clones cannot reuse existing computer accounts in Active Directory.
- Persona Management is not available.
- 3D rendering is not available.
- You cannot specify a minimum number of ready (provisioned) machines during instant-clone maintenance operations. This feature is not needed because the high speed of creating instant clones means that some desktops are always available even during maintenance operations.

The disk space reclamation feature that is available to View Composer linked clones is not needed because instant clones are recreated when users log out. For instant clones, reclaiming unused disk space in a VM does not have a significant impact on storage consumption.

Image Publishing and Rebalancing an Instant-Clone Desktop Pool

The clones in an instant-clone desktop pool are based on the same image. When an instant clone is created, the desktop pool are rebalanced across datastores automatically.

An image is a snapshot of a parent VM. Creating an instant-clone desktop pool involves the following operations:

1 View publishes the image that you select. In vCenter Server, four folders (`ClonePrepInternalTemplateFolder`, `ClonePrepParentVmFolder`, `ClonePrepReplicaVmFolder`, and `ClonePrepResyncVmFolder`) are created if they do not exist, and some internal VMs that are required for cloning are created. In View Administrator, you can see the progress of this operation on the **Summary** tab of the desktop pool. During publishing, the Pending Image pane shows the name and state of the image.

   NOTE Do not tamper with the four folders or the internal VMs that they contain. Otherwise, errors might occur. The internal VMs are removed when they are no longer needed. Normally the VMs are removed within 5 minutes of pool deletion or a push-image operation. However, sometimes the removal can take up to 30 minutes.

2 The clones are created. This process is fast. Typically, a clone can be created in less than 2 seconds. During this process, the Current Image pane in View Administrator shows the name and state of the image.

After the pool is created, you can change the image through the push-image operation. See "Change the Image of an Instant-Clone Desktop Pool" in the *View Administration* document. As with the creation of a pool, the new image is first published. Then the clones are recreated.

If you edit a pool to add or remove datastores, rebalancing of the VMs happens automatically when a new clone is created. If you want rebalancing to happen faster, take the following actions:

- If you remove a datastore, manually remove the desktops on that datastore so that the new desktops are created on the remaining datastores.
- If you add a datastore, manually remove some desktops from the original datastores so that the new desktops are created on the new datastore. You can also remove all desktops or simply do a push image with the same image so that when the clones are recreated, they are evenly distributed across the datastores.

Add an Instant-Clone Domain Administrator

Before you create an instant-clone desktop pool, you must add an instant-clone domain administrator to View.

The instant-clone domain administrator must have certain Active Directory domain privileges. For more information, see "Create a User Account for Instant-Clone Operations" in the *View Installation* document.

Procedure

1 In View Administrator, select **View Configuration > Instant Clone Domain Admins**.

2 Click **Add**.

3 Enter the login name and password for of the instant-clone domain administrator.

Worksheet for Creating an Instant-Clone Desktop Pool

When you create an instant-clone desktop pool, the Add Desktop Pool wizard prompts you to configure certain options. You can use this worksheet to record your configuration options before you create the pool.

Before creating an instant-clone desktop pool, take a snapshot of the parent VM. You must shut down the parent VM before taking the snapshot. The snapshot is the base image for the clones.

Note You cannot create an instant-clone desktop pool from a VM template.

Table 7‑1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool

Option	Description	Fill In Your Value Here
User assignment	Select **Floating**. Users are assigned random desktops from the pool.	
vCenter Server	Select **Instant clones** and select the vCenter Server that manages the instant-clone VMs.	
Desktop Pool ID	The unique name that identifies the pool in View Administrator. If you have multiple Connection Server configurations, make sure that another Connection Server configuration does not use the same pool ID. A Connection Server configuration can consist of a single Connection Server or multiple Connection Servers	
Display name	The pool name that users see when they log in from a client. If you do not specify a name, the pool ID is used.	
Access group	Select an access group for the pool, or leave the pool in the default root access group. If you use an access group, you can delegate managing the pool to an administrator who has a specific role. For details, see the role-based delegated administration chapter in the *View Administration* document. **Note** Access groups are different from vCenter Server folders that store desktop VMs. You select a vCenter Server folder later in the wizard.	
State	If set to **Enabled**, the pool is ready for use after provisioning. If set to **Disabled**, the pool is not available to users. During provisioning, if you disable the pool, provisioning stops.	
Connection Server restrictions	You can restrict access to the pool to certain Connection Servers by clicking **Browse** and selecting one or more Connection Servers. If you intend to provide access to desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager app might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.	
Automatically logoff after disconnect	■ **Immediately**. Users are logged off when they disconnect. ■ **Never**. Users are never logged off. ■ **After**. The time after which users are logged off when they disconnect. Type the duration in minutes. The logoff time applies to future disconnections. If a desktop session is already disconnected when you set a logoff time, the logoff duration for that user starts when you set the logoff time, not when the session was originally disconnected. For example, if you set this value to 5 minutes, and a session was disconnected 10 minutes earlier, View will log off that session 5 minutes after you set the value.	
Allow user to initiate separate sessions from different client devices	With this option selected, a user connecting to the same desktop pool from different client devices gets different desktop sessions. The user can only reconnect to an existing session from the same client device. When this setting is not selected, users are always reconnected to their existing session no matter which client device is used.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Default display protocol	Select the default display protocol. The choices are **Microsoft RDP**, **PCoIP**, and **VMware Blast**.	
Allow users to choose protocol	Specify whether users can choose display protocols other than the default. Do not allow users to choose a display protocol.	
3D Renderer	Select 3D graphics rendering for desktops. 3D rendering is supported on Windows 7 or later guests running on VMs with virtual hardware version 8 or later. The hardware-based renderer is supported (at minimum) on virtual hardware version 9 in a vSphere 5.1 environment. The software renderer is supported (at minimum) on virtual hardware version 8 in a vSphere 5.0 environment. On ESXi 5.0 hosts, the renderer allows a maximum VRAM size of 128MB. On ESXi 5.1 and later hosts, the maximum VRAM size is 512MB. On hardware version 11 (HWv11) virtual machines in vSphere 6.0, the VRAM value (video memory) has changed. Select the Manage Using vSphere Client option and configure video memory for these machines in vSphere Web Client. For details, see "Configuring 3D Graphics" in the vSphere Virtual Machine Administration guide. 3D rendering is disabled if you select Microsoft RDP as the default display protocol and do not allow users to choose a display protocol. ■ **NVIDIA GRID vGPU**. 3D rendering is enabled for NVIDIA GRID vGPU. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. See, "Preparing for NVIDIA GRID vGPU Capabilities" in the *Setting Up Virtual Desktops in Horizon 7* document. You cannot use vSphere Distributed Resource Scheduler (DRS) when you select this option. An instant-clone desktop pool configured to use NVIDIA GRID vGPU fails to start virtual desktops in the pool with the PCoIP display protocol. You can use the Blast Extreme display protocol to start the virtual desktops in the instant-clone desktop pool configured with NVIDIA GRID vGPU. ■ **Disabled**. 3D rendering is inactive. Default is disabled.	
HTML Access	Select **Enabled** to allow users to connect to remote desktops from a Web browser. For more information about this feature, see *Using HTML Access*, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html . To use HTML Access with VMware Identity Manager, you must pair Connection Server with a SAML authentication server, as described in the *View Administration* document. VMware Identity Manager must be installed and configured for use with Connection Server.	
Adobe Flash quality	Select the quality of Adobe Flash content on Web pages. ■ **Do not control**. The Web page settings determine the quality. ■ **Low**. This setting consumes the least amount of bandwidth. If no quality level is specified, this is the default level. ■ **Medium**. This setting consumes a moderate amount of bandwidth. ■ **High**. This setting consumes the most amount of bandwidth. For more information, see "Adobe Flash Quality and Throttling," on page 111.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Adobe Flash throttling	Select the frame rate of Adobe Flash movies. If you enable this setting, you can reduce or increase the number of frames displayed per second by selecting the throttling level. ■ **Disabled**. No throttling is performed. ■ **Conservative**. Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames. ■ **Moderate**. Timer interval is 500 milliseconds. ■ **Aggressive**. Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames. For more information, see "Adobe Flash Quality and Throttling," on page 111.	
Stop provisioning on error	Specify whether View stops provisioning desktop VMs if an error occurs and prevents the error from affecting multiple VMs.	
Naming pattern	Specify a pattern that View uses as a prefix in all the desktop VM names, followed by a unique number. For more information, see "Using a Naming Pattern for Automated Desktop Pools," on page 102.	
Max number of machines	Specify the total number of desktop VMs in the pool.	
Number of spare (powered on) machines	Specify the number of desktop VMs to keep available to users. For details, see "Naming Machines Manually or Providing a Naming Pattern," on page 100.	
Provision machines on demand Min number of machines Provision all machines up front	Specify whether to provision all desktop VMs when the pool is created or to provision the VMs when they are needed. ■ **Provision all machines up front**. When the pool is created, View provisions the number of VMs you specify in **Max number of machines**. ■ **Provision machines on demand**. When the pool is created, View creates the number of VMs based on the **Min number of machines** value or the **Number of spare (powered on) machines** value, whichever is higher. Additional VMs are created to maintain this minimum number of available VMs as users connect to desktops.	
Select separate datastores for replica and OS disks	Specify whether to store the replica and OS disks on a datastore that is different from the datastores that the instant clones are on. If you select this option, you can select the options to select one or more instant-clone datastores or replica disk datastores. For more information, see "Storing Replicas and Clones on Separate Datastores for Instant Clones and View Composer Linked Clones," on page 155.	
Parent VM	Select the parent VM for the pool.	
Snapshot (default image)	Select the snapshot of the parent VM to use as the base image for the pool.	
VM folder location	Select the folder in vCenter Server for the desktop VMs.	
Cluster	Select the vCenter Server cluster for the desktop VMs.	
Resource pool	Select the vCenter Server resource pool for the desktop VMs.	
Datastores	Select one or more datastores for the desktop VMs. The Select Instant Clone Datastores window provides high-level guidelines for estimating the pool's storage requirements. These guidelines help you determine which datastores are large enough to store the clones. The Storage Overcommit value is always set to Unbounded and is not configurable.	

Table 7-1. Worksheet: Configuration Options for Creating an Instant-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Replica disk datastores	Select one or more replica disk datastores on which to store the instant-clones. This option appears if you select separate datastores for replica and OS disks. A table on the Select Replica Disk Datastores page of the Add Farm wizard provides high-level guidelines for estimate the farm's storage requirements. These guidelines can help you determine which replica disk datastores are enough to store the instant-clones.	
Networks	Select the networks to use for the instant-clone desktop pool. You can select multiple vLAN networks to create a larger instant-clone desktop pool. The default setting uses the network from the current parent VM image. A table on the Select Networks wizard provides the networks, ports, and port bindings that are available to use. To use multiple networks, you must unselect **Use network from current parent VM** and then select the networks to use with the instant-clone farm.	
vGPU Profile	Select a vGPU profile from the list of profiles supported by vGPU for the selected cluster. Mixed vGPU profiles on a single ESXi cluster are not supported. After a pool is provisioned, you cannot edit the vGPU profile. To change the vGPU profile, you must delete the pool and create a new pool with the desired vGPU profile. During the pool creation process, the administrator must select a vGPU profile that matches the vGPU profile on the master VM. If the administrator cannot recall the vGPU profile of the master VM, the administrator must locate the correct snapshot to find the vGPU profile. If the administrator selects the wrong vGPU profile, the pool creation will fail.	
Domain	Select an Active Directory domain. The drop-down list shows the domains that you specify when you configure instant-clone domain administrators. See "Add an Instant-Clone Domain Administrator," on page 83	
AD container	Specify the Active Directory container's relative distinguished name. For example: **`CN=Computers`** In the Add Desktop Pool window, you can browse the Active Directory tree for the container.	
Power-off script	Specify the path name of a script to run on the desktop VMs and the script parameters before the VMs are powered off.	
Post-synchronization script	Specify the path name of a script to run on the desktop VMs and the script parameters after the VMs are created.	

Create an Instant-Clone Desktop Pool

The Add Desktop Pool wizards guides you through the steps of creating an instant-clone desktop pool.

Prerequisites

- Verify that the virtual switch that the instant-clone VMs connect to has enough ports to support the expected number of VMs. Each network card on a VM requires one port.
- Verify that you have a parent VM ready. For more information, see Chapter 4, "Creating and Preparing a Parent Virtual Machine for Cloning," on page 19.
- Gather the configuration information for the pool. See "Worksheet for Creating an Instant-Clone Desktop Pool," on page 84.

- Verify that you added an instant-clone domain administrator in View Administrator. See "Add an Instant-Clone Domain Administrator," on page 83.

Procedure

1. In View Administrator, select **Catalog > Desktop Pools**.
2. Click **Add**.
3. Select **Automated Desktop Pool**.
4. On the vCenter Server page, select **Instant clones**.
5. Follow the prompts to create the pool.

   Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page by clicking the page name in the navigation pane.

In View Administrator, you can view the desktop VMs as they are added to the pool by selecting **Catalog > Desktop Pools**.

After you create the pool, do not delete the parent VM or remove it from the vCenter Server inventory as long as the pool exists. If you remove the VM from the vCenter Server inventory by mistake, you must add it back and then do a push image using the current image.

What to do next

Entitle users to access the pool. See "Add Entitlements to a Desktop or Application Pool," on page 131.

ClonePrep Guest Customization

ClonePrep customizes instant clones during the creation process.

ClonePrep ensures that all instant clones join an Active Directory domain. The clones have the same computer security identifiers (SIDs) as the parent VM. ClonePrep also preserves the globally unique identifiers (GUIDs) of applications, although some applications might generate a new GUID during customization.

When you add an instant-clone desktop pool, you can specify a script to run immediately after a clone is created and another script to run before the clone is powered off.

How ClonePrep Runs Scripts

ClonePrep uses the Windows `CreateProcess` API to run scripts. Your script can invoke any process that can be created with the `CreateProcess` API. For example, `cmd`, `vbscript`, `exe`, and batch-file processes work with the API.

Specifically, ClonePrep passes the path of the script as the second parameter to the `CreateProcess` API and sets the first parameter to `NULL`. For example, if the script path is `c:\myscript.cmd`, the call to `CreateProcess` is `CreateProcess(NULL,c:\myscript.cmd,...)`.

Providing Paths to ClonePrep Scripts

You can specify the scripts when you create or edit the desktop pool. The scripts must reside on the parent VM. You cannot use a UNC path to a network share.

If you use a scripting language that needs an interpreter to run the script, the script path must start with the interpreter executable. For example, instead of specifying `C:\script\myvb.vbs`, you must specify `C:\windows\system32\cscript.exe c:\script\myvb.vbs`.

IMPORTANT Put the ClonePrep customization scripts in a secure folder to prevent unauthorized access.

ClonePrep Script Timeout Limit

By default, ClonePrep terminates a script if the execution takes longer than 20 seconds. You can increase this timeout limit. For details, see "Increase the Timeout Limit for ClonePrep and QuickPrep Customization Scripts," on page 49.

Alternatively, you can specify a script that runs another script or process that takes a long time to run.

ClonePrep Script Account

ClonePrep runs the scripts using the same account that the VMware Horizon Instant Clone Agent service uses. By default, this account is Local System. Do not change this login account. If you do, the clones will fail to start.

ClonePrep Process Privileges

For security reasons, certain Windows operating system privileges are removed from the VMware Horizon Instant Clone Agent process that runs ClonePrep customization scripts. The scripts cannot perform actions that require those privileges.

The process that runs ClonePrep scripts do not have the following privileges:

- SeCreateTokenPrivilege
- SeTakeOwnershipPrivilege
- SeSecurityPrivilege
- SeSystemEnvironmentPrivilege
- SeLoadDriverPrivilege
- SeSystemtimePrivilege
- SeUndockPrivilege
- SeManageVolumePrivilege
- SeLockMemoryPrivilege
- SeIncreaseBasePriorityPrivilege
- SeCreatePermanentPrivilege
- SeDebugPrivilege
- SeAuditPrivilege

ClonePrep Script Logs

ClonePrep writes messages to a log file. The log file is `C:\Windows\Temp\vmware-viewcomposer-ga-new.log`.

Perform Maintenance on Instant-Clone VMs

You can perform maintenance on instant-clone VMs by putting the ESXi hosts into maintenance mode. You can also use the instant-clone maintenance utilities to perform manual maintenance on instant-clone VMs.

To use the instant-clone utilities, see "Instant-Clone Maintenance Utilities," on page 90.

You can use vSphere Web Client to put the ESXi host into maintenance mode. The ESX host maintenance operation automatically deletes the parent VMs from that ESXi host.

Note After the ESXi host is put into maintenance, you must wait approximately five minutes before performing any actions on instant clones after the ESXi host performs entering or exiting operations.

Procedure

1 Log in to vSphere Web Client.

2 Select the ESXi host that you want to put into maintenance and click**Maintenance Mode > Enter Maintenance Mode**.

Instant-Clone Maintenance Utilities

On the Connection Server are two utilities that you can use for the maintenance of instant-clone VMs in vCenter Server and the clusters that the VMs are in.

The utilities are `IcMaint.cmd` and `IcUnprotect.cmd` and are located in `C:\Program Files\VMware\VMware View\Server\tools\bin`.

IcMaint.cmd

This command deletes the parent VMs from the ESXi host so that the host can be put into maintenance mode. The host is not automatically put into maintenance mode. To perform maintenance on the host, the vCenter server administrator must manually put the host into maintenance mode.

Syntax:

```
IcMaint.cmd –vc hostname_or_IP_address –uid user_ID –password password –hostName ESXi_hostname –
maintenance ON|OFF
```

Parameters:

- `–vc` *host name or IP address of vCenter Server*
- `–uid` *vCenter Server user ID*
- `–password` *vCenter Server user password*
- `–hostname` *ESXi host name*
- `–maintenance` `ON|OFF`

  This parameter specifies whether the host is available for hosting parent VMs.

  After the command is run on the host, the InstantClone.Maintenance annotation value is set to 1 and the parent VMs are deleted. After the parent VMs are deleted, the InstantClone.Maintenance annotation value is set to 2 and no more parent VMs are created on the host. When you run this command again with `–maintenanceOFF`, the InstantClone.Maintenance annotation value is cleared for the host to become available for hosting parent VMs.

All the parameters are required.

IcUnprotect.cmd

This utility unprotects the folders and VMs that ClonePrep creates. ClonePrep is the mechanism that customizes instant clones during the creation process.

Syntax:

```
IcUnprotect.cmd –vc hostname_or_IP_address –uid user_ID –password password [–clusterId
cluster_ID] [–includeFolders]
```

Parameters:

- `-vc` *host name or IP address of vCenter Server*
- `-uid` *vCenter Server user ID*
- `-password` *vCenter Server user password*
- `-clusterId` *cluster ID*
- `-includeFolders`

  This parameter unprotects the folders in addition to the VMs.

All the parameters are required except `clusterId` and `includeFolders`. If `clusterId` is not specified, protection is removed from all ClonePrep VMs in all data centers.

Creating Manual Desktop Pools 8

In a manual desktop pool, each remote desktop that is accessed by an end user is a separate machine. When you create a manual desktop pool, you select existing machines. You can create a pool that contains a single desktop by creating a manual desktop pool and selecting a single machine.

This chapter includes the following topics:

Manual Desktop Pools

To create a manual desktop pool, View provisions desktops from existing machines. You select a separate machine for each desktop in the pool.

View can use several types of machines in manual pools:

- Virtual machines that are managed by vCenter Server
- Virtual machines that run on a virtualization platform other than vCenter Server
- Physical computers

For information about creating a manual desktop pool that uses Linux virtual machines, see the *Setting Up Horizon 7 for Linux Desktops* guide.

Worksheet for Creating a Manual Desktop Pool

When you create a manual desktop pool, the View Administrator Add Desktop Pool wizard prompts you to configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

You can print this worksheet and write down the values you want to specify when you run the Add Desktop Pool wizard.

Note In a manual pool, you must prepare each machine to deliver remote desktop access. Horizon Agent must be installed and running on each machine.

Table 8-1. Worksheet: Configuration Options for Creating a Manual Desktop Pool

Option	Description	Fill In Your Value Here
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a machine. Users receive the same machine each time they log in. ■ In a floating-assignment pool, users receive different machines each time they log in. For details, see "User Assignment in Desktop Pools," on page 99.	
vCenter Server	The vCenter Server that manages the machines. This option appears only if the machines are virtual machines that are managed by vCenter Server.	
Machine Source	The virtual machines or physical computers that you want to include in the desktop pool. 1 Decide which type of machine you want to use. You can use either virtual machines that are managed by vCenter Server or unmanaged virtual machines and physical computers. 2 Prepare a list of the vCenter Server virtual machines or unmanaged virtual machines and physical computers that you want to include in the desktop pool. 3 Install Horizon Agent on each machine that you want to include in the desktop pool. To use PCoIP with machines that are unmanaged virtual machines or physical computers, you must use Teradici hardware. **NOTE** When you enable Windows Server desktops in View Administrator, View Administrator displays all available Windows Server machines, including machines on which View Connection Server and other View servers are installed, as potential machine sources. You cannot select machines for the desktop pool if View server software is installed on the machines. Horizon Agent cannot coexist on the same virtual or physical machine with any other View software component, including View Connection Server, security server, View Composer, or Horizon Client.	
Desktop Pool ID	The pool name that users see when they log in and that identifies the pool in View Administrator. If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID.	

Table 8-1. Worksheet: Configuration Options for Creating a Manual Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Desktop Pool Settings	Settings that determine the machine state, power status when a virtual machine is not in use, display protocol, Adobe Flash quality, and so on. For details, see "Desktop Pool Settings for All Desktop Pool Types," on page 107. For a list of the settings that apply to manual pools, see "Desktop Pool Settings for Manual Pools," on page 97.	
Transparent Page Sharing Scope	Select the level at which to allow transparent page sharing (TPS). The choices are **Virtual Machine** (the default), **Pool**, **Pod**, or **Global**. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications. Page sharing happens on the ESXi host. For example, if you enable TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by Horizon 7 on the same ESXi host can share memory pages, regardless of which pool the machines reside in. **Note** The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.	

Create a Manual Desktop Pool

You can create a manual desktop pool that provisions desktops from existing virtual machines or physical computers. You must select the machines that will be included in the desktop pool.

For manual pools with virtual machines that are managed by vCenter Server, View ensures that a spare machine is powered on so that users can connect to it. The spare machine is powered on no matter which power policy is in effect.

Prerequisites

- Prepare the machines to deliver remote desktop access. In a manual pool, you must prepare each machine individually. Horizon Agent must be installed and running on each machine.

  To prepare virtual machines managed by vCenter Server, see Chapter 4, "Creating and Preparing a Parent Virtual Machine for Cloning," on page 19.

  To prepare unmanaged virtual machines and physical computers, see Chapter 3, "Preparing Unmanaged Machines," on page 15.

- Gather the configuration information that you must provide to create the pool. See "Worksheet for Creating a Manual Desktop Pool," on page 93.

- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See "Desktop Pool Settings for All Desktop Pool Types," on page 107.

Procedure

1 In View Administrator, select **Catalog > Desktop Pools**.

2 Click **Add**.

3 Select **Manual Desktop Pool**.

4 Follow the prompts in the wizard to create the pool.

   Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

In View Administrator, you can view the machines as they are added to the pool by selecting **Catalog > Desktop Pools**.

What to do next

Entitle users to access the pool. See "Add Entitlements to a Desktop or Application Pool," on page 131.

Create a Manual Pool That Contains One Machine

You can create a pool that contains a single machine when a user requires a unique, dedicated desktop, or when, at different times, multiple users must access a costly application with a single-host license.

You can provision an individual machine in its own pool by creating a manual desktop pool and selecting a single machine.

To mimic a physical computer that can be shared by multiple users, specify a floating assignment for the users entitled to access the pool.

Whether you configure the single-machine pool with dedicated or floating assignment, power operations are initiated by session management. The virtual machine is powered on when a user requests the desktop and powered off or suspended when the user logs off.

If you configure the **Ensure machines are always powered on** policy, the virtual machine remains powered on. If the user shuts down the virtual machine, it immediately restarts.

Prerequisites

- Prepare the machine to deliver remote desktop access. Horizon Agent must be installed and running on the machine.

  To prepare a virtual machine managed by vCenter Server, see Chapter 4, "Creating and Preparing a Parent Virtual Machine for Cloning," on page 19.

  To prepare an unmanaged virtual machine or physical computer, see Chapter 3, "Preparing Unmanaged Machines," on page 15.

- Gather the configuration information you must provide to create the manual pool. See "Worksheet for Creating a Manual Desktop Pool," on page 93.

- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See "Desktop Pool Settings for All Desktop Pool Types," on page 107.

Procedure

1 In View Administrator, select **Catalog > Desktop Pools**.

2 Click **Add**.

3 Select **Manual Desktop Pool**.

4 Select the type of user assignment.

Option	Description
Dedicated	The machine is assigned to one user. Only that user can log in to the desktop.
Floating	The machine is shared by all users who are entitled to the pool. Any entitled user can log in to the desktop as long as another user is not logged in.

5 On the Machine Source page, select the machine to be included in the desktop pool.

6 Follow the prompts in the wizard to create the pool.

Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page you completed by clicking the page name in the navigation panel.

In View Administrator, you can view the machine being added to the pool by selecting **Catalog > Desktop Pools**.

What to do next

Entitle users to access the pool. See "Add Entitlements to a Desktop or Application Pool," on page 131.

Desktop Pool Settings for Manual Pools

You must specify machine and pool settings when you configure manual desktop pools. Not all settings apply to all types of manual pools.

Table 8-2 lists the settings that apply to manual desktop pools that are configured with these properties:

- Dedicated user assignments
- Floating user assignments
- Managed machines (vCenter Server virtual machines)
- Unmanaged machines

These settings also apply to a manual pool that contains a single machine.

For descriptions of each desktop pool setting, see "Desktop Pool Settings for All Desktop Pool Types," on page 107.

Table 8-2. Settings for Manual Desktop Pools

Setting	Manual Managed Pool, Dedicated Assignment	Manual Managed Pool, Floating Assignment	Manual Unmanaged Pool, Dedicated Assignment	Manual Unmanaged Pool, Floating Assignment
State	Yes	Yes	Yes	Yes
Connection Server restrictions	Yes	Yes	Yes	Yes
Remote machine power policy	Yes	Yes		
Automatically logoff after disconnect	Yes	Yes	Yes	Yes
Allow users to reset/restart their machines	Yes	Yes		

Table 8-2. Settings for Manual Desktop Pools (Continued)

Setting	Manual Managed Pool, Dedicated Assignment	Manual Managed Pool, Floating Assignment	Manual Unmanaged Pool, Dedicated Assignment	Manual Unmanaged Pool, Floating Assignment
Allow user to initiate separate sessions from different client devices		Yes		Yes
Default display protocol	Yes	Yes	Yes To use PCoIP with a machine that is not managed by vCenter Server, you must install Teradici hardware on the machine.	Yes To use PCoIP with a machine that is not managed by vCenter Server, you must install Teradici hardware on the machine.
Allow users to choose protocol	Yes	Yes	Yes	Yes
3D Renderer	Yes	Yes		
Max number of monitors	Yes	Yes		
Max resolution of any one monitor	Yes	Yes		
Adobe Flash quality	Yes	Yes	Yes	Yes
Adobe Flash throttling	Yes	Yes	Yes	Yes
Override global Mirage settings	Yes	Yes	Yes	Yes
Mirage Server configuration	Yes	Yes	Yes	Yes

Provisioning Desktop Pools 9

When you create a desktop pool, you select configuration options that determine how the pool is managed and how users interact with the desktops.

These provisioning tasks apply to desktop pools that are deployed on single-user machines. They do not apply to RDS desktop pools. However, the Adobe Flash quality and throttling settings apply to all types of desktop pools, including RDS.

This chapter includes the following topics:

User Assignment in Desktop Pools

For manual desktop pools and automated desktop pools of full virtual machines or View Composer linked clones, you can choose floating or dedicated user assignment for the desktops. For instant-clone desktop pools, you can choose only floating user assignment.

With a dedicated assignment, each desktop is assigned to a specific user. A user logging in for the first time gets a desktop that is not assigned to another user. Thereafter, this user will always get this desktop after logging in, and this desktop is not available to any other user.

With a floating assignment, users get a random desktop every time they log in. When a user logs off, the desktop is returned to the pool.

With instant clones, the desktop is always deleted and recreated from the current image when a user logs out. With View Composer linked clones, you can configure floating-assignment machines to be deleted when users log out. Automatic deletion lets you keep only as many virtual machines as you need at one time.

With floating-assignment, you might be able to reduce software licensing costs.

Naming Machines Manually or Providing a Naming Pattern

With an automated desktop pool of full virtual machines or View Composer linked clones, you can specify a list of names for the desktop machines or provide a naming pattern. With an instant-clone desktop pool, you can only specify a naming pattern when provisioning the pool.

If you name machines by specifying a list, you can use your company's naming scheme, and you can associate each machine name with a user.

If you provide a naming pattern, View can dynamically create and assign machines as users need them.

Table 9-1 compares the two naming methods, showing how each method affects the way you create and administer a desktop pool.

Table 9-1. Naming machines Manually or Providing a machine-Naming Pattern

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
Machine names	The machine names are generated by appending a number to the naming pattern. For details, see "Using a Naming Pattern for Automated Desktop Pools," on page 102.	You specify a list of machine names. In a dedicated-assignment pool, you can pair users with machines by listing user names with the machine names. For details, see "Specify a List of Machine Names," on page 101.
Pool size	You specify a maximum number of machines.	Your list of machine names determines the number of machines.
To add machines to the pool	You can increase the maximum pool size.	You can add machine names to the list. For details, see "Add Machines to an Automated Pool Provisioned by a List of Names," on page 104.
On-demand provisioning	Available. View dynamically creates and provisions the specified minimum and spare number of machines as users first log in or as you assign machines to users. View can also create and provision all the machines when you create the pool.	Not available. View creates and provisions all the machines that you specify in your list when the pool is created.
Initial customization	Available. When a machine is provisioned, View can run a customization specification that you select.	Available. When a machine is provisioned, View can run a customization specification that you select.
Manual customization of dedicated machines	Not available to instant clones. To customize machines and return desktop access to your users, you must remove and reassign the ownership of each machine. Depending on whether you assign machines on first log in, you might have to perform these steps twice. You cannot start machines in maintenance mode. After the pool is created, you can manually put the machines into maintenance mode.	You can customize and test machines without having to reassign ownership. When you create the pool, you can start all machines in maintenance mode to prevent users from accessing them. You can customize the machines and exit maintenance mode to return access to your users. For details, see "Manually Customizing Machines," on page 105.

Table 9-1. Naming machines Manually or Providing a machine-Naming Pattern (Continued)

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
Dynamic or fixed pool size	Dynamic. If you remove a user assignment from a machine in a dedicated-assignment pool, the machine is returned to the pool of available machines. If you choose to delete machines on logoff in a floating-assignment pool, the pool size can grow or shrink depending on the number of active user sessions. NOTE Instant-clone pools can only be floating-assignment pools. The machines are always deleted on logoff.	Fixed. The pool contains the number of machines you provide in the list of machine names. You cannot select the **Delete machine on logoff** setting if you name machines manually.
Spare machines	You can specify a number of spare machines that View keeps powered on for new users. View creates new machines to maintain the specified number. View stops creating spare machines when it reaches the maximum pool size. View keeps the spare machines powered on even when the pool power policy is **Power off** or **Suspend**, or when you do not set a power policy. NOTE Instant-clone pools do not have a power policy.	You can specify a number of spare machines that View keeps powered on for new users. View does not create new spare machines to maintain the specified number. View keeps the spare machines powered on even when the pool power policy is **Power off** or **Suspend**, or when you do not set a power policy.
User assignment	You can use a naming pattern for dedicated-assignment and floating-assignment pools. NOTE Instant-clone pools can only be floating-assignment pools.	You can specify machine names for dedicated-assignment and floating-assignment pools. NOTE In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Specify a List of Machine Names

You can provision an automated desktop pool by manually specifying a list of machine names. This naming method lets you use your company's naming conventions to identify the machines in a pool.

When you explicitly specify machine names, users can see familiar names based on their company's organization when they log in to their remote desktops.

Follow these guidelines for manually specifying machine names:

- Type each machine name on a separate line.
- A machine name can have up to 15 alphanumeric characters.
- You can add a user name to each machine entry. Use a comma to separate the user name from the machine name.

In this example, two machines are specified. The second machine is associated with a user:

```
Desktop-001
Desktop-002,abccorp.com\jdoe
```

Note In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Prerequisites

Make sure that each machine name is unique. You cannot use the names of existing virtual machines in vCenter Server.

Procedure

1 Create a text file that contains the list of machine names.

   If you intend to create a desktop pool with only a few machines, you can type the machine names directly in the Add Desktop Pool wizard. You do not have to create a separate text file.

2 In View Administrator start the Add Desktop Pool wizard to begin creating an automated desktop pool.

3 On the Provisioning Settings page, select **Specify names manually** and click **Enter names**.

4 Copy your list of machine names in the Enter Machine Names page and click **Next**.

   The Enter Machine Names wizard displays the desktop list and indicates validation errors with a red **!**.

5 Correct invalid machine names.

   a Place your cursor over an invalid name to display the related error message at the bottom of the page.

   b Click **Back**.

   c Edit the incorrect names and click **Next**.

6 Click **Finish**.

7 (Optional) Select **Start machines in maintenance mode**.

   This option lets you customize the machines before users can log in and use them.

8 Follow the prompts in the wizard to finish creating the desktop pool.

View creates a machine for each name in the list. When an entry includes a machine and user name, View assigns the machine to that user.

After the desktop pool is created, you can add machines by importing another list file that contains additional machine names and users. See "Add Machines to an Automated Pool Provisioned by a List of Names" in the *View Administration* document.

Using a Naming Pattern for Automated Desktop Pools

You can provision the machines in a pool by providing a naming pattern and the total number of machines you want in the pool. By default, View uses your pattern as a prefix in all the machine names and appends a unique number to identify each machine.

Length of the Naming Pattern in a Machine Name

Machine names have a 15-character limit, including your naming pattern and the automatically generated number.

Table 9-2. Maximum Length of the Naming Pattern in a Machine Name

If You Set This Number of Machines in the Pool	This Is the Maximum Prefix Length
1-99	13 characters
100-999	12 characters
1,000 or more	11 characters

Names that contain fixed-length tokens have different length limits. See "Length of the Naming Pattern When You Use a Fixed-Length Token," on page 103.

Using a Token in a Machine Name

You can place the automatically generated number anywhere else in the name by using a token. When you type the pool name, type **n** surrounded by curly brackets to designate the token.

For example: **amber-{n}-desktop**

When a machine is created, View replaces **{n}** with a unique number.

You can generate a fixed-length token by typing **{n:fixed=*number of digits*}**.

View replaces the token with numbers containing the specified number of digits.

For example, if you type **amber-{n:fixed=3}**, View replaces **{n:fixed=3}** with a three-digit number and creates these machine names: **amber-001**, **amber-002**, **amber-003**, and so on.

Length of the Naming Pattern When You Use a Fixed-Length Token

Names that contain fixed-length tokens have a 15-character limit, including your naming pattern and the number of digits in the token.

Table 9-3. Maximum Length of the Naming Pattern When You Use a Fixed-Length Token

Fixed-Length Token	Maximum Length of the Naming Pattern
{n:fixed=1}	14 characters
{n:fixed=2}	13 characters
{n:fixed=3}	12 characters

Machine-Naming Example

This example shows how to create two automated desktop pools that use the same machine names, but different sets of numbers. The strategies that are used in this example achieve a specific user objective and show the flexibility of the machine-naming methods.

The objective is to create two pools with the same naming convention such as VDIABC-*XX*, where *XX* represents a number. Each pool has a different set of sequential numbers. For example, the first pool might contain machines VDIABC-01 through VDIABC-10. The second pool contains machines VDIABC-11 through VDIABC-20.

You can use either machine-naming method to satisfy this objective.

- To create fixed sets of machines at one time, specify machine names manually.
- To create machines dynamically when users log in for the first time, provide a naming pattern and use a token to designate the sequential numbers.

Specifying the Names Manually

1 Prepare a text file for the first pool that contains a list of machine names from VDIABC-01 through VDIABC-10.

2 In View Administrator, create the pool and specify machine names manually.

3 Click **Enter Names** and copy your list into the **Enter Machine Names** list box.

4 Repeat these steps for the second pool, using the names VDIABC-11 through VDIABC-20.

For detailed instructions, see "Specify a List of Machine Names," on page 101.

You can add machines to each pool after it is created. For example, you can add machines VDIABC-21 through VDIABC-30 to the first pool, and VDIABC-31 through VDIABC-40 to the second pool. See "Add Machines to an Automated Pool Provisioned by a List of Names," on page 104.

Providing a Naming Pattern With a Token

1 In View Administrator, create the first pool and use a naming pattern to provision the machine names.

2 In the naming-pattern text box, type **`VDIABC-0{n}`**.

3 Limit the pool's maximum size to 9.

4 Repeat these steps for the second pool, but in the naming-pattern text box, type **`VDIABC-1{n}`**.

The first pool contains machines VDIABC-01 through VDIABC-09. The second pool contains machines VDIABC-11 through VDIABC-19.

Alternatively, you can configure the pools to contain up to 99 machines each by using a fixed-length token of 2 digits:

- For the first pool, type **`VDIABC-0{n:fixed=2}`**.
- For the second pool, type **`VDIABC-1{n:fixed=2}`**.

Limit each pool's maximum size to 99. This configuration produces machines that contain a 3-digit sequential naming pattern.

First pool:

```
VDIABC-001
VDIABC-002
VDIABC-003
```

Second pool:

```
VDIABC-101
VDIABC-102
VDIABC-103
```

For details about naming patterns and tokens, see "Using a Naming Pattern for Automated Desktop Pools," on page 102.

Add Machines to an Automated Pool Provisioned by a List of Names

To add machines to an automated desktop pool provisioned by manually specifying machine names, you provide another list of new machine names. This feature lets you expand a desktop pool and continue to use your company's naming conventions.

In Horizon 7.0, this feature is not supported for instant clones.

Follow these guidelines for manually adding machine names:

- Type each machine name on a separate line.
- A machine name can have up to 15 alphanumeric characters.
- You can add a user name to each machine entry. Use a comma to separate the user name from the machine name.

In this example, two machines are added. The second machine is associated with a user:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

Note In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

Prerequisites

Verify that you created the desktop pool by manually specifying machine names. You cannot add machines by providing new machine names if you created the pool by providing a naming pattern.

Procedure

1 Create a text file that contains the list of additional machine names.

If you intend to add only a few machines, you can type the machine names directly in the Add Desktop Pool wizard. You do not have to create a separate text file.

2 In View Administrator, select **Catalog > Desktop Pools**.

3 Select the desktop pool to be expanded.

4 Click **Edit**.

5 Click the **Provisioning Settings** tab.

6 Click **Add Machines**.

7 Copy your list of machine names in the Enter Machine Names page and click **Next**.

The Enter Machine Names wizard displays the machine list and indicates validation errors with a red **X**.

8 Correct invalid machine names.

a Place your cursor over an invalid name to display the related error message at the bottom of the page.

b Click **Back**.

c Edit the incorrect names and click **Next**.

9 Click **Finish**.

10 Click **OK**.

In vCenter Server, you can monitor the creation of the new virtual machines.

In View Administrator, you can view the machines as they are added to the desktop pool by selecting **Catalog > Desktop Pools**.

Manually Customizing Machines

After you create an automated pool, you can customize particular machines without reassigning ownership. By starting the machines in maintenance mode, you can modify and test the machines before you release them to users.

Note This feature is not available to an instant-clone desktop pool.

Customizing Machines in Maintenance Mode

Maintenance mode prevents users from accessing their desktops. If you start machines in maintenance mode, View places each machine in maintenance mode when the machine is created.

In a dedicated-assignment pool, you can use maintenance mode to log in to a machine without having to reassign ownership to your own administrator account. When you finish the customization, you do not have to return ownership to the user assigned to the machine.

In a floating-assignment pool, you can test machines in maintenance mode before you let users log in.

To perform the same customization on all machines in an automated pool, customize the virtual machine you prepare as a template or parent. View deploys your customization to all the machines. When you create the pool, you can also use a Sysprep customization specification to configure all the machines with licensing, domain attachment, DHCP settings, and other computer properties.

NOTE You can start machines in maintenance mode if you manually specify machine names for the pool, not if you name machines by providing a naming pattern.

Customize Individual Machines

You can customize individual machines after a pool is created by starting the machines in maintenance mode.

Procedure

1. In View Administrator, begin creating an automated desktop pool by starting the Add Desktop Pool wizard.
2. On the Provisioning Settings page, select **Specify names manually**.
3. Select **Start machines in maintenance mode**.
4. Complete the Add Desktop Pool wizard to finish creating the desktop pool.
5. In vCenter Server, log in, customize, and test the individual virtual machines.

   You can customize the machines manually or by using standard Windows systems-management software such as Altiris, SMS, LanDesk, or BMC.
6. In View Administrator, select the desktop pool.
7. Use the filter tool to select specific machines to release to your users.
8. Click **More Commands > Exit Maintenance Mode**.

What to do next

Notify your users that they can log in to their desktops.

Desktop Pool Settings for All Desktop Pool Types

You must specify machine and desktop pool settings when you configure automated pools that contain full virtual machines, linked-clone desktop pools, manual desktop pools, instant-clone desktop pools, and RDS desktop pools. Not all settings apply to all types of desktop pools.

Table 9-4. Desktop Pool Setting Descriptions

Setting	Options
State	■ **Enabled**. After being created, the desktop pool is enabled and ready for immediate use. ■ **Disabled**. After being created, the desktop pool is disabled and unavailable for use, and provisioning is stopped for the pool. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance. When this state is in effect, remote desktops are unavailable for use.
Connection Server restrictions	■ **None**. The desktop pool can be accessed by any Connection Server instance. ■ **With tags**. Select one or more Connection Server tags to make the desktop pool accessible only to Connection Server instances that have those tags. You can use the check boxes to select multiple tags. If you intend to provide access to your desktops through VMware Identity Manager, and you configure Connection Server restrictions, the VMware Identity Manager app might display desktops to users when those desktops are actually restricted. VMware Identity Manager users will be unable to launch these desktops.
Remote machine power policy	Determines how a virtual machine behaves when the user logs off of the associated desktop. For descriptions of the power-policy options, see "Power Policies for Desktop Pools," on page 112. For more information about how power policies affect automated pools, see "Setting Power Policies for Desktop Pools," on page 112. Not applicable to instant-clone desktop pools. Instant clones are always powered on.
Automatically logoff after disconnect	■ **Immediately**. Users are logged off as soon as they disconnect. ■ **Never**. Users are never logged off. ■ **After**. The time after which users are logged off when they disconnect. Type the duration in minutes. The log off time applies to future disconnections. If a desktop session was already disconnected when you set a log off time, the log off duration for that user starts when you set the log off time, not when the session was originally disconnected. For example, if you set this value to five minutes, and a session was disconnected 10 minutes earlier, View will log off that session five minutes after you set the value.
Allow users to reset/restart their machines	Allow users to reset or restart their own desktops.
Allow user to initiate separate sessions from different client devices	When this setting is selected, a user connecting to the same desktop pool from different client devices will get different desktop sessions. The user can only reconnect to an existing session from the client device where that session was initiated. When this setting is not selected, the user will be reconnected to his or her existing session no matter which client device is used.
Delete machine after logoff	Select whether to delete floating-assignment, full virtual machines. ■ **No**. Virtual machines remain in the desktop pool after users log off. ■ **Yes**. Virtual machines are powered off and deleted as soon as users log off. For instant-clone desktops, the machine is always deleted and recreated after logoff.

Table 9-4. Desktop Pool Setting Descriptions (Continued)

Setting	Options
Delete or refresh machine on logoff	Select whether to delete, refresh, or leave alone floating-assignment, linked-clone virtual machines. ■ **Never**. Virtual machines remain in the pool and are not refreshed after users log off. ■ **Delete immediately**. Virtual machines are powered off and deleted as soon as users log off. When users log off, virtual machines immediately go into a `Deleting` state. ■ **Refresh immediately**. Virtual machines are refreshed as soon as users log off. When users log off, virtual machines immediately go into maintenance mode to prevent other users from logging in as the refresh operation begins. For instant-clone desktops, the machine is always deleted and recreated after logoff.
Refresh OS disk after logoff	Select whether and when to refresh the OS disks for dedicated-assignment, linked-clone virtual machines. ■ **Never**. The OS disk is never refreshed. ■ **Always**. The OS disk is refreshed every time the user logs off. ■ **Every**. The OS disk is refreshed at regular intervals of a specified number of days. Type the number of days. The number of days is counted from the last refresh, or from the initial provisioning if no refresh has occurred yet. For example, if the specified value is **3** days, and three days have passed since the last refresh, the machine is refreshed after the user logs off. ■ **At**. The OS disk is refreshed when its current size reaches a specified percentage of its maximum allowable size. The maximum size of a linked clone's OS disk is the size of the replica's OS disk. Type the percentage at which refresh operations occur. With the **At** option, the size of the linked clone's OS disk in the datastore is compared to its maximum allowable size. This disk-utilization percentage does not reflect disk usage that you might see inside the machine's guest operating system. When you refresh the OS disks in a linked-clone pool with dedicated assignment, the View Composer persistent disks are not affected. For instant-clone desktops, the machine is always deleted and recreated after logoff.
Default display protocol	Select the display protocol that you want Connection Server to use to communicate with clients. **VMware Blast**: The VMware Blast Extreme protocol is built on the H.264 protocol and supports the broadest range of client devices, including smart phones, tablets, ultra-low-cost PCs, and Macs, across any network. This protocol consumes the least CPU resources and so provides longer battery life on mobile devices. **PCoIP**: The default option wherever it is supported. PCoIP is supported as the display protocol for virtual and physical machines that have Teradici hardware. PCoIP provides an optimized PC experience for the delivery of images, audio, and video content for a wide range of users on the LAN or across the WAN. **Microsoft RDP**: Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a computer remotely.
Allow users to choose protocol	Allow users to override the default display protocol for their desktops by using Horizon Client.

Table 9-4. Desktop Pool Setting Descriptions (Continued)

Setting	Options
3D Renderer	You can select whether to enable 3D graphics rendering if your pool comprises Windows 7 or later desktops. You can configure the **3D Renderer** to use software rendering or hardware rendering based on physical GPU graphics cards installed on ESXi 5.1 or later hosts. To enable this feature, you must select PCoIP or VMware Blast as the protocol and disable the **Allow users to choose protocol** setting (select **No**). With the hardware-based **3D Renderer** options, users can take advantage of graphics applications for design, modeling, and multimedia. With the software **3D Renderer** option, users can take advantage of graphics enhancements in less demanding applications such as AERO, Microsoft Office, and Google Earth. For system requirements, see "Configuring 3D Rendering for Desktops," on page 117. If your View deployment does not run on vSphere 5.0 or later, this setting is not available and is inactive in View Administrator. When you select this feature, if you select the **Automatic**, **Software**, or **Hardware** option, you can configure the amount of VRAM that is assigned to machines in the pool. The maximum number of monitors is 2 and the maximum resolution is 1920 x 1200. If you select **Manage using vSphere Client**, or **NVIDIA GRID vGPU**, you must configure the amount of 3D memory and the number of monitors in vCenter Server. You can select at most four monitors for your machines that are used as remote desktops, depending on the monitor resolution. **Note** When you configure or edit this setting, you must power off existing virtual machines, verify that the machines are reconfigured in vCenter Server, and power on the machines to cause the new setting to take effect. Restarting a virtual machine does not cause the new setting to take effect. For more information, see "Configuring 3D Rendering for Desktops," on page 117, "3D Renderer Options," on page 120. and "Best Practices for Configuring 3D Rendering," on page 122. For instant-clone desktop pools, NVIDIA GRID vGPU is the only 3D Renderer option available.
Max number of monitors	If you select PCoIP or VMware Blast as the display protocol, you can select the **Maximum number of monitors** on which users can display the desktop. You can select up to four monitors. When the **3D Renderer** setting is not selected, the **Max number of monitors** setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the number of monitors, more memory is consumed on the associated ESXi hosts. When the **3D Renderer** setting is not selected, up to three monitors are supported at 3840 x 2160 resolution on a Windows 7 guest operating system with Aero disabled. For other operating systems, or for Windows 7 with Aero enabled, one monitor is supported at 3840 x 2160 resolution. When the **3D Renderer** setting is selected, one monitor is supported at 3840 x 2160 resolution. Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution. **Note** You must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect. Not available to instant-clone desktop pools. In Horizon 7.0 the maximum number of monitors for instant clones is 2.

Table 9-4. Desktop Pool Setting Descriptions (Continued)

Setting	Options
Max resolution of any one monitor	If you select PCoIP or VMware Blast as the display protocol, you should specify the **Maximum resolution of any one monitor**. The **Maximum resolution of any one monitor** is set to 1920 x 1200 pixels by default, but you can configure this value. When the **3D Renderer** setting is not selected, the **Max resolution of any one monitor** setting affects the amount of VRAM that is assigned to machines in the pool. When you increase the resolution, more memory is consumed on the associated ESXi hosts. When the **3D Renderer** setting is not selected, up to three monitors are supported at 3840 x 2160 resolution on a Windows 7 guest operating system with Aero disabled. For other operating systems, or for Windows 7 with Aero enabled, one monitor is supported at 3840 x 2160 resolution. When the **3D Renderer** setting is selected, one monitor is supported at 3840 x 2160 resolution. Multiple monitors are best supported at a lower resolution. Select fewer monitors if you select a higher resolution. **Note** You must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect. Not available to instant-clone desktop pools. In Horizon 7.0, the maximum resolution of any monitor is 2560 x 1600.
HTML Access	Select **Enabled** to allow users to connect to remote desktops from within their Web browsers. When a user logs in through the VMware Horizon Web portal page or the VMware Identity Manager app and selects a remote desktop, the HTML Access agent enables the user to connect to the desktop over HTTPS. The desktop is displayed in the user's browser. Other display protocols, such as PCoIP or RDP, are not used. Horizon Client software does not have to be installed on the client devices. To use HTML Access, you must install HTML Access in your View deployment. For more information, see *Using HTML Access*, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html. To use HTML Access with VMware Identity Manager, you must pair Connection Server with a SAML Authentication server, as described in the *View Administration* document. VMware Identity Manager must be installed and configured for use with Connection Server.
Adobe Flash quality	Determines the quality of Adobe Flash content that is displayed on Web pages. ■ **Do not control**. Quality is determined by Web page settings. ■ **Low**. This setting results in the most bandwidth savings. If no quality level is specified, the system defaults to Low. ■ **Medium**. This setting results in moderate bandwidth savings. ■ **High**. This setting results in the least bandwidth savings. For more information, see "Adobe Flash Quality and Throttling," on page 111.
Adobe Flash throttling	Determines the frame rate of Adobe Flash movies. If you enable this setting, you can reduce or increase the number of frames displayed per second by selecting an aggressiveness level. ■ **Disabled**. No throttling is performed. The timer interval is not modified. ■ **Conservative**. Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames. ■ **Moderate**. Timer interval is 500 milliseconds. ■ **Aggressive**. Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames. For more information, see "Adobe Flash Quality and Throttling," on page 111.

Table 9-4. Desktop Pool Setting Descriptions (Continued)

Setting	Options
Override global Mirage settings	To specify the same Mirage server for all desktop pools, use the global View configuration setting rather than this pool-specific setting. Not available to instant-clone desktop pools.
Mirage Server configuration	Allows you to specify the URL of a Mirage server, using the format **`mirage://`*`server-name`*`:`*`port`*** or **`mirages://`*`server-name`*`:`*`port`***. Here *server-name* is the fully qualified domain name. If you do not specify the port number, the default port number 8000 is used. Specifying the Mirage server in View Administrator is an alternative to specifying the Mirage server when installing the Mirage client. To find out which versions of Mirage support having the server specified in View Administrator, see the Mirage documentation, at https://www.vmware.com/support/pubs/mirage_pubs.html. Not available to instant-clone desktop pools.

Adobe Flash Quality and Throttling

You can specify a maximum allowable level of quality for Adobe Flash content that overrides Web page settings. If Adobe Flash quality for a Web page is higher than the maximum level allowed, quality is reduced to the specified maximum. Lower quality results in more bandwidth savings.

To make use of Adobe Flash bandwidth-reduction settings, Adobe Flash must not be running in full screen mode.

Table 9-5 shows the available Adobe Flash render-quality settings.

Table 9-5. Adobe Flash Quality Settings

Quality Setting	Description
Do not control	Quality is determined by Web page settings.
Low	This setting results in the most bandwidth savings.
Medium	This setting results in moderate bandwidth savings.
High	This setting results in the least bandwidth savings.

If no maximum level of quality is specified, the system defaults to a value of **Low**.

Adobe Flash uses timer services to update what is shown on the screen at a given time. A typical Adobe Flash timer interval value is between 4 and 50 milliseconds. By throttling, or prolonging, the interval, you can reduce the frame rate and thereby reduce bandwidth.

Table 9-6 shows the available Adobe Flash throttling settings.

Table 9-6. Adobe Flash Throttling Settings

Throttling Setting	Description
Disabled	No throttling is performed. The timer interval is not modified.
Conservative	Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames.
Moderate	Timer interval is 500 milliseconds.
Aggressive	Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames.

Audio speed remains constant regardless of which throttling setting you select.

Setting Power Policies for Desktop Pools

You can configure a power policy for the virtual machines in a desktop pool if the virtual machines are managed by vCenter Server except instant clones.

Power policies control how a virtual machine behaves when its associated desktop is not in use. A desktop is considered not in use before a user logs in and after a user disconnects or logs off. Power policies also control how a virtual machine behaves after administrative tasks such as refresh, recompose, and rebalance are completed.

You configure power policies when you create or edit desktop pools in Horizon Administrator.

Note You cannot configure power policies for desktop pools that have unmanaged machines or instant clones. Instant clones are always powered on.

Power Policies for Desktop Pools

Power policies control how a virtual machine behaves when the associated remote desktop is not in use.

You set power policies when you create or edit a desktop pool. Table 9-7 describes the available power policies.

Table 9-7. Power Policies

Power Policy	Description
Take no power action	View does not enforce any power policy after a user logs off. This setting has two consequences. ■ View does not change the power state of the virtual machine after a user logs off. For example, if a user shuts down the virtual machine, the virtual machine remains powered off. If a user logs off without shutting down, the virtual machine remains powered on. When a user reconnects to the desktop, the virtual machine restarts if it was powered off. ■ View does not enforce any power state after an administrative task is completed. For example, a user might log off without shutting down. The virtual machine remains powered on. When a scheduled recomposition takes place, the virtual machine is powered off. After the recomposition is completed, View does nothing to change the power state of the virtual machine. It remains powered off.
Ensure machines are always powered on	The virtual machine remains powered on, even when it is not in use. If a user shuts down the virtual machine, it immediately restarts. The virtual machine also restarts after an administrative task such as refresh, recompose, or rebalance is completed. Select **Ensure machines are always powered on** if you run batch processes or system management tools that must contact the virtual machines at scheduled times.

Table 9-7. Power Policies (Continued)

Power Policy	Description
Suspend	The virtual machine enters a suspended state when a user logs off, but not when a user disconnects. You can also configure machines in a dedicated pool to be suspended when a user disconnects without logging off. To configure this policy, you must set an attribute in View LDAP. See "Configure Dedicated Machines To Be Suspended After Users Disconnect," on page 114. When multiple virtual machines are resumed from a suspended state, some virtual machines might have delays in powering on. Whether any delays occur depends on the ESXi host hardware and the number of virtual machines that are configured on an ESXi host. Users connecting to their desktops from Horizon Client might temporarily see a desktop-not-available message. To access their desktops, users can connect again.
Power off	The virtual machine shuts down when a user logs off, but not when a user disconnects.

Note When you add a machine to a manual pool, View powers on the machine to ensure that it is fully configured, even when you select the **Power off** or **Take no power action** power policy. After Horizon Agent is configured, it is marked as Ready, and the normal power-management settings for the pool apply.

For manual pools with machines that are managed by vCenter Server, View ensures that a spare machine is powered on so that users can connect to it. The spare machine is powered on no matter which power policy is in effect.

Table 9-8 describes when View applies the configured power policy.

Table 9-8. When View Applies the Power Policy

Desktop Pool Type	The power policy is applied ...
Manual pool that contains one machine (vCenter Server-managed virtual machine)	Power operations are initiated by session management. The virtual machine is powered on when a user requests the desktop and powered off or suspended when the user logs off. **Note** The **Ensure machines are always powered on** policy always applies, whether the single-machine pool uses floating or dedicated assignment, and whether the machine is assigned or unassigned.
Automated pool with dedicated assignment	To unassigned machines only. On assigned machines, power operations are initiated by session management. Virtual machines are powered on when a user requests an assigned machine and are powered off or suspended when the user logs off. **Note** The **Ensure machines are always powered on** policy applies to assigned and unassigned machines.
Automated pool with floating assignment	When a machine is not in use and after a user logs off. When you configure the **Power off** or **Suspend** power policy for a floating-assignment desktop pool, set **Automatically logoff after disconnect** to **Immediately** to prevent discarded or orphaned sessions.

Table 9-8. When View Applies the Power Policy (Continued)

Desktop Pool Type	The power policy is applied ...
Manual pool with dedicated assignment	To unassigned machines only. On assigned machines, power operations are initiated by session management. Virtual machines are powered on when a user requests an assigned machine and are powered off or suspended when the user logs off. NOTE The **Ensure machines are always powered on** policy applies to assigned and unassigned machines.
Manual pool with floating assignment	When a machine is not in use and after a user logs off. When you configure the **Power off** or **Suspend** power policy for a floating-assignment desktop pool, set **Automatically logoff after disconnect** to **Immediately** to prevent discarded or orphaned sessions.

How View applies the configured power policy to automated pools depends on whether a machine is available. See "How Power Policies Affect Automated Desktop Pools," on page 114 for more information.

Configure Dedicated Machines To Be Suspended After Users Disconnect

The **Suspend** power policy causes virtual machines to be suspended when a user logs off, but not when a user disconnects. You can also configure machines in a dedicated pool to be suspended when a user disconnects from a desktop without logging off. Using suspend when users disconnect helps to conserve resources.

To enable suspend on disconnect for dedicated machines, you must set an attribute in View LDAP.

Procedure

1. Start the ADSI Edit utility on your View Connection Server host.
2. In the console tree, select **Connect to**.
3. In the **Select or type a domain or server** field, type the server name as `localhost:389`
4. Under **Connection point**, click **Select or type a distinguished name or naming context**, type the distinguished name as `DC=vdi,DC=vmware,DC=int`, and click **OK**.

   The ADAM ADSI Edit main window appears.
5. Expand the ADAM ADSI tree and expand **OU=Properties**.
6. Select **OU=Global** and select **CN=Common** in the right pane
7. Select **Action > Properties**, and under the **pae-NameValuePair** attribute, add the new entry `suspendOnDisconnect=1`.
8. Restart the VMware Horizon View Connection Server service or View Connection Server.

How Power Policies Affect Automated Desktop Pools

How View applies the configured power policy to automated pools depends on whether a machine is available.

A machine in an automated pool is considered available when it meets the following criteria:

- Is active
- Does not contain a user session
- Is not assigned to a user

The Horizon Agent service running on the machine confirms the availability of the machine to View Connection Server.

When you configure an automated pool, you can specify the minimum and maximum number of virtual machines that must be provisioned and the number of spare machines that must be kept powered on and available at any given time.

Power Policy Examples for Automated Pools with Floating Assignments

When you configure an automated pool with floating assignments, you can specify that a particular number of machines must be available at a given time. The spare, available machines are always powered on, no matter how the pool policy is set.

Power Policy Example 1

Table 9-9 describes the floating-assignment, automated pool in this example. The pool uses a machine-naming pattern to provision and name the machines.

Table 9-9. Desktop Pool Settings for Automated Pool with Floating Assignment Example 1

Desktop Pool Setting	Value
Number of machines (minimum)	10
Number of machines (maximum)	20
Number of spare, powered-on machines	2
Remote machine power policy	Power off

When this desktop pool is provisioned, 10 machines are created, two machines are powered on and immediately available, and eight machines are powered off.

For each new user that connects to the pool, a machine is powered on to maintain the number of spare, available machines. When the number of connected users exceeds eight, additional machines, up to the maximum of 20, are created to maintain the number of spare machines. After the maximum number is reached, the machines of the first two users who disconnect remain powered on to maintain the number of spare machines. The machine of each subsequent user is powered off according to the power policy.

Power Policy Example 2

Table 9-10 describes the floating-assignment, automated pool in this example. The pool uses a machine-naming pattern to provision and name the machines.

Table 9-10. Desktop Pool Settings for Automated Pool with Floating Assignments Example 2

Desktop Pool Setting	Value
Number of machines (minimum)	5
Number of machines (maximum)	5
Number of spare, powered-on machines	2
Remote machine power policy	Power off

When this desktop pool is provisioned, five machines are created, two machines are powered on and immediately available, and three machines are powered off.

If a fourth machine in this pool is powered off, one of the existing machines is powered on. An additional machine is not powered on because the maximum of number of machines has already been reached.

Power Policy Example for Automated Pools with Dedicated Assignments

Unlike a powered-on machine in an automated pool with floating assignments, a powered-on machine in an automated pool with dedicated assignments is not necessarily available. It is available only if the machine is not assigned to a user.

Table 9-11 describes the dedicated-assignment, automated pool in this example.

Table 9-11. Desktop Pool Settings for Automated Pool with Dedicated Assignments Example

Desktop Pool Setting	Value
Number of machines (minimum)	3
Number of machines (maximum)	5
Number of spare, powered-on machines	2
Remote machine power policy	Ensure machines are always powered on

When this desktop pool is provisioned, three machines are created and powered on. If the machines are powered off in vCenter Server, they are immediately powered on again, according to the power policy.

After a user connects to a machine in the pool, the machine becomes permanently assigned to that user. After the user disconnects from the machine, the machine is no longer available to any other user. However, the **Ensure machines are always powered on** policy still applies. If the assigned machine is powered off in vCenter Server, it is immediately powered on again.

When another user connects, a second machine is assigned. Because the number of spare machines falls below the limit when the second user connects, another machine is created and powered on. An additional machine is created and powered on each time a new user is assigned until the maximum machine limit is reached.

Preventing View Power Policy Conflicts

When you use View Administrator to configure a power policy, you must compare the power policy to the settings in the guest operating system's Power Options control panel to prevent power policy conflicts.

A virtual machine can become temporarily inaccessible if the power policy configured for the machine is not compatible with a power option configured for the guest operating system. If there are other machines in the same pool, they can also be affected.

The following configuration is an example of a power policy conflict:

- In View Administrator, the power policy **Suspend** is configured for the virtual machine. This policy causes the virtual machine to enter a suspended state when it is not in use.
- In the Power Options control panel in the guest operating system, the option **Put the Computer to sleep** is set to three minutes.

In this configuration, both View Connection Server and the guest operating system can suspend the virtual machine. The guest operating system power option might cause the virtual machine to be unavailable when View Connection Server expects it to be powered on.

Configuring 3D Rendering for Desktops

When you create or edit a desktop pool of virtual machines, you can configure 3D graphics rendering for your desktops. Desktops can take advantage of Virtual Shared Graphics Acceleration (vSGA), Virtual Dedicated Graphics Acceleration (vDGA), or shared GPU hardware acceleration (NVIDIA GRID vGPU). vDGA and NVIDIA GRID vGPU are vSphere features that use physical graphics cards installed on the ESXi hosts and manage the graphics processing unit (GPU) resources among the virtual machines.

Note This feature is not available to instant clones in Horizon 7.0.

End users can take advantage of 3D applications for design, modeling, and multimedia, which typically require GPU hardware to perform well. For users that do not require physical GPU, a software option provides graphics enhancements that can support less demanding applications such as Windows AERO, Microsoft Office, and Google Earth. Following are brief descriptions of the 3D graphics options:

NVIDIA GRID vGPU (shared GPU hardware acceleration)

Available with vSphere 6.0 and later, this feature allows a physical GPU on an ESXi host to be shared among virtual machines. This feature offers flexible hardware-accelerated 3D profiles ranging from lightweight 3D task workers to high-end workstation graphics power users.

AMD Multiuser GPU using vDGA

Available with vSphere 6.0 and later, this feature allows multiple virtual machines to share an AMD GPU by making the GPU appear as multiple PCI passthrough devices. This feature offers flexible hardware-accelerated 3D profiles, ranging from lightweight 3D task workers to high-end workstation graphics power users.

Virtual Dedicated Graphics Acceleration (vDGA)

Available with vSphere 5.5 and later, this feature dedicates a single physical GPU on an ESXi host to a single virtual machine. Use this feature if you require high-end, hardware-accelerated workstation graphics.

Note Some Intel vDGA cards require a certain vSphere 6 version. See the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

Virtual Shared Graphics Acceleration (vSGA)

Available with vSphere 5.1 and later, this feature allows multiple virtual machines to share the physical GPUs on ESXi hosts. This feature is suitable for mid-range 3D design, modeling, and multimedia applications.

Soft 3D

Software-accelerated graphics, available with vSphere 5.0 and later, allows you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical GPU. Use this feature for less demanding 3D applications such as Windows Aero themes, Microsoft Office 2010, and Google Earth.

Because NVIDIA GRID vGPU, AMD Multiuser GPU using vDGA, and all vDGA solutions use PCI pass-through on the ESXi host, live VMotion is not supported. vSGA and Soft 3D support live VMotion.

In some cases, if an application such as a video game or 3D benchmark forces the desktop to display in full screen resolution, the desktop session can be disconnected. Possible workarounds include setting the application to run in Windowed mode or matching the View session desktop resolution to the default resolution expected by the application.

Requirements for All Types of 3D Rendering

To enable 3D graphics rendering, your pool deployment must meet the following requirements:

- The virtual machines must be Windows 7 or later.
- The pool can use PCoIP, VMware Blast Extreme, or RDP as the default display protocol.
- 3D rendering settings are disabled when the default display protocol is set to RDP and users are not allowed to choose a protocol.

IMPORTANT When you configure or edit the **3D Renderer** setting, you must power off existing virtual machines, verify that the machines are reconfigured in vCenter Server, and power on the machines to cause the new setting to take effect. Restarting a virtual machine does not cause the new setting to take effect.

Additional Requirements for NVIDIA GRID vGPU

With NVIDIA GRID vGPU, a single physical GPU on an ESXi host can be shared among virtual machines. To support this type of shared GPU hardware acceleration, a pool must meet these additional requirements:

- The virtual machines must run on ESXi 6.0 or later hosts, be virtual hardware version 11 or later, and be managed by vCenter Server 6.0 or later software.

  You must configure the parent virtual machine or the virtual machine template to use a shared PCI device before you create the desktop pool in View. For detailed instructions, see the NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1.

- You must install graphics drivers from the GPU vendor in the guest operating system of the virtual machine.

  NOTE For a list of supported GPU hardware, see the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php.

- You must set the **3D Renderer** option in Horizon Administrator to **NVIDIA GRID vGPU**.
- NVIDIA GRID vGPU enabled instant-clone desktop pools are supported for vSphere 2016 and later.

Additional Requirements for AMD Multiuser GPU using vDGA

With AMD Multiuser GPU using vDGA, multiple virtual machines to share an AMD GPU by making the GPU appear as multiple PCI passthrough devices. To support this type of shared GPU hardware acceleration, a pool must meet these additional requirements:

- The virtual machines must run on ESXi 6.0 or later hosts, be virtual hardware version 11 or later, and be managed by vCenter Server 6.0 or later software.
- You must enable GPU pass-through on the ESXi hosts, configure AMD SR-IOV (Single Root I/O Virtualization), and configure the individual virtual machines to use dedicated PCI devices. See "Preparing to Use the Capabilities of AMD Multiuser GPU Using vDGA," on page 126.

  NOTE Only manual desktop pools are supported for this release.

- You must install graphics drivers from the GPU vendor in the guest operating system of the virtual machine.

  NOTE For a list of supported GPU hardware, see the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php.

- You must set the **3D Renderer** option in View Administrator to **Manage using vSphere Client**.

Additional Requirements for Using vDGA

vDGA dedicates a single physical GPU on an ESXi host to a single virtual machine. To support vDGA, a pool must meet these additional requirements:

- The virtual machines must run on ESXi 5.5 or later hosts, be virtual hardware version 9 or later, and be managed by vCenter Server 5.5 or later software.

  You must enable GPU pass-through on the ESXi hosts and configure the individual virtual machines to use dedicated PCI devices after the desktop pool is created in View. You cannot configure the parent virtual machine or template for vDGA and then create a desktop pool, because the same physical GPU would be dedicated to every virtual machine in the pool. See "vDGA Installation" in the VMware white paper about graphics acceleration.

  For linked-clone virtual machines, vDGA settings are preserved after refresh, recompose, and rebalance operations.

- You must install graphics drivers from the GPU vendor in the guest operating system of the virtual machine.

  Note For a list of supported GPU hardware, see the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php.

- You must set the **3D Renderer** option to **Manage using vSphere Client**.

Additional Requirements for Using vSGA

vSGA allows multiple virtual machines to share the physical GPUs on ESXi hosts. To support vSGA, a pool must meet these additional requirements:

- The virtual machines must run on ESXi 5.1 or later hosts and be managed by vCenter Server 5.1 or later software.

- GPU graphics cards and the associated vSphere Installation Bundles (VIBs) must be installed on the ESXi hosts. For a list of supported GPU hardware, see the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php.

- Windows 7 machines must be virtual hardware version 8 or later. Windows 8 machines must be virtual hardware version 9 or later. Windows 10 machines must be virtual hardware version 10 or later.

- You can set the **3D Renderer** option to any of the following settings: **Manage using vSphere Client**, **Automatic**, or **Hardware**. See also "Video RAM Configuration Options for the 3D Renderer," on page 120.

  Automatic uses hardware acceleration if there is a capable and available hardware GPU in the ESXi host. If a hardware GPU is not available, the virtual machine uses software 3D rendering for any 3D tasks.

Additional Requirements for Using Soft 3D

To support software 3D rendering, a pool must meet these additional requirements:

- The virtual machines must run on ESXi 5.0 or later hosts and be managed by vCenter Server 5.0 or later software.

- The machines must be virtual hardware version 8 or later.

- You must set the **3D Renderer** option to **Software**. See also "Video RAM Configuration Options for the 3D Renderer," on page 120.

Video RAM Configuration Options for the 3D Renderer

When you enable the **3D Renderer** setting, if you select the **Automatic**, **Software**, or **Hardware** option, you can configure the amount of VRAM that is assigned to the virtual machines in the pool by moving the slider in the Configure VRAM for 3D guests dialog box. The minimum VRAM size is 64MB. The default VRAM amount depends on the virtual hardware version:

- For virtual hardware version 8 (vSphere 5.0) virtual machines, the default VRAM size is 64MB, and you can configure a maximum size of 128MB.
- For virtual hardware version 9 (vSphere 5.1) and 10 (vSphere 5.5 Update 1) virtual machines, the default VRAM size is 96MB, and you can configure a maximum size of 512MB.
- For virtual hardware version 11 (vSphere 6.0) virtual machines, the default VRAM size is 96MB, and you can configure a maximum size of 128MB. In vSphere 6.0 and later virtual machines, this setting refers only to the amount of display memory in the graphics card and therefore has a lower maximum setting than earlier virtual hardware versions, which included both display memory and guest memory for storing 3D objects.

The VRAM settings that you configure in View Administrator take precedence over the VRAM settings that can be configured for the virtual machines in vSphere Client or vSphere Web Client, unless you select the **Manage using vSphere Client** option.

For more information about the **Automatic**, **Software**, or **Hardware** 3D rendering options, see "3D Renderer Options," on page 120.

3D Renderer Options

The **3D Renderer** setting for desktop pools provides options that let you configure graphics rendering in different ways.

The following table describes the differences between the various types of 3D rendering options available in View Administrator but does not provide complete information for configuring virtual machines and ESXi hosts for Virtual Shared Graphics Acceleration (vSGA), Virtual Dedicated Graphics Acceleration (vDGA), AMD Multiuser GPU Using vDGA, and NVIDIA GRID vGPU. These tasks must be done with vSphere Web Client before you attempt to create desktop pools in View Administrator. For instructions about these tasks for vSGA and vDGA, see the VMware white paper about graphics acceleration. For instructions about NVIDIA GRID vGPU, see the NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1. For instructions about AMD Multiuser GPU Using vDGA, see the "Preparing to Use the Capabilities of AMD Multiuser GPU Using vDGA," on page 126.

Table 9-12. 3D Renderer Options for Pools Running on vSphere 5.1 or Later

Option	Description
Manage using vSphere Client	The **3D Renderer** option that is set in vSphere Web Client (or vSphere Client in vSphere 5.1 or later) for a virtual machine determines the type of 3D graphics rendering that takes place. View does not control 3D rendering. In the vSphere Web Client, you can configure the **Automatic**, **Software**, or **Hardware** options. These options have the same effect as they do when you set them in View Administrator. Use this setting when configuring vDGA and AMD Multiuser GPU Using vDGA. This setting is also an option for vSGA. When you select the **Manage using vSphere Client** option, the **Configure VRAM for 3D Guests**, **Max number of monitors**, and **Max resolution of any one monitor** settings are inactive in View Administrator. You can configure the amount of memory in vSphere Web Client.
Automatic	3D rendering is enabled. The ESXi host controls the type of 3D rendering that takes place. For example, the ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. If all GPU hardware resources are already reserved when a virtual machine is powered on, ESXi uses the software renderer for that machine. This setting is an option when configuring vSGA. The ESXi host allocates VRAM to a virtual machine based on the value that is set in the Configure VRAM for 3D Guests dialog box.
Software	3D rendering is enabled. The ESXi host uses software 3D graphics rendering. If a GPU graphics card is installed on the ESXi host, this pool will not use it. Use this setting to configure Soft 3D. The ESXi host allocates VRAM to a virtual machine based on the value that is set in the Configure VRAM for 3D Guests dialog box.
Hardware	3D rendering is enabled. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. This setting is an option when configuring vSGA. The ESXi host allocates VRAM to a virtual machine based on the value that is set in the Configure VRAM for 3D Guests dialog box. IMPORTANT If you configure the **Hardware** option, consider these potential constraints: ■ If a user tries to connect to a machine when all GPU hardware resources are reserved, the virtual machine will not power on, and the user will receive an error message. ■ If you use vMotion to move the machine to an ESXi host that does not have GPU hardware configured, the virtual machine will not power on. When you configure hardware-based 3D rendering, you can examine the GPU resources that are allocated to each virtual machine on an ESXi host. For details, see "Examining GPU Resources on an ESXi Host," on page 128.

Table 9-12. 3D Renderer Options for Pools Running on vSphere 5.1 or Later (Continued)

Option	Description
NVIDIA GRID vGPU	3D rendering is enabled for NVIDIA GRID vGPU . The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. If a user tries to connect to a machine when all GPU hardware resources are being used by other virtual machines on the host, View Connection Server will attempt to move the virtual machine to another ESXi host in the cluster before powering on. Use this setting when configuring NVIDIA GRID vGPU. When you select the **NVIDIA GRID vGPU** option, the **Configure VRAM for 3D Guests**, **Max number of monitors**, and **Max resolution of any one monitor** settings are inactive in View Administrator. When you configure the parent virtual machine or virtual machine template with vSphere Web Client, you are prompted to reserve all memory. IMPORTANT If you configure the **NVIDIA GRID vGPU** option, consider these potential constraints: ■ The virtual machine cannot be suspended or resumed. Therefore the Remote Machine Power Policy option for suspending the virtual machine is not available. ■ If you use vMotion to move the machine to an ESXi host that does not have GPU hardware configured, the virtual machine will not power on. Live vMotion is not available. ■ All ESXi hosts in the cluster must be version 6.0 or later, and the virtual machines must be hardware version 11 or later. ■ If an ESXi cluster contains a host that is NVIDIA GRID vGPU enabled and a host that is not NVIDIA GRID vGPU enabled, the hosts display a yellow (warning) status in the View Administrator Dashboard. If a user tries to connect to a machine when all GPU hardware resources are being used by other virtual machines on the host, View Connection Server will attempt to move the virtual machine to another ESXi host in the cluster before powering on. In this case, hosts that are not NVIDIA GRID vGPU enabled cannot be used for this type of dynamic migration.
Disabled	3D rendering is inactive.

Table 9-13. 3D Renderer Options for Pools Running on vSphere 5.0

Option	Description
Enabled	The **3D Renderer** option is enabled. The ESXi host uses software 3D graphics rendering. When software rendering is configured, the default VRAM size is 64MB, the minimum size. In the Configure VRAM for 3D Guests dialog box, you can use the slider to increase the amount of VRAM that is reserved. With software rendering, the ESXi host allocates up to a maximum of 128MB per virtual machine. If you set a higher VRAM size, it is ignored.
Disabled	3D rendering is inactive.

If a desktop pool is running on earlier vSphere version than 5.0, the **3D Renderer** setting is inactive and is not available in View Administrator.

Best Practices for Configuring 3D Rendering

The 3D rendering options and other pool settings offer various advantages and drawbacks. Select the option that best supports your vSphere hardware infrastructure and your users' requirements for graphics rendering.

NOTE This topic provides an overview of the controls you find in View Administrator. For detailed information about all the various choices and requirements for 3D rendering, see the VMware white paper about graphics acceleration.

When to Choose the Automatic Option

The **Automatic** option is the best choice for many View deployments that require 3D rendering. vSGA (Virtual Shared Graphics Acceleration)-enabled virtual machines can dynamically switch between software and hardware 3D rendering, without your having to reconfigure. This option ensures that some type of 3D rendering takes place even when GPU resources are completely reserved. In a mixed cluster of ESXi 5.1 and ESXi 5.0 hosts, this option ensures that a virtual machine is powered on successfully and uses 3D rendering even if, for example, vMotion moved the virtual machine to an ESXi 5.0 host.

The only drawback with the **Automatic** option is that you cannot easily tell whether a virtual machine is using hardware or software 3D rendering.

When to Choose the Hardware Option

The **Hardware** option guarantees that every virtual machine in the pool uses hardware 3D rendering, provided that GPU resources are available on the ESXi hosts. This option might be the best choice when all your users run graphically intensive applications. You can use this option when configuring vSGA (Virtual Shared Graphics Acceleration).

With the **Hardware** option, you must strictly control your vSphere environment. All ESXi hosts must be version 5.1 or later and must have GPU graphics cards installed.

When all GPU resources on an ESXi host are reserved, View cannot power on a virtual machine for the next user who tries to log in to a desktop. You must manage the allocation of GPU resources and the use of vMotion to ensure that resources are available for your desktops.

When to Choose the Option to Manage Using vSphere Client

When you select the **Manage using vSphere Client** option, you can use vSphere Web Client to configure individual virtual machines with different options and VRAM values.

- For vSGA (Virtual Shared Graphics Acceleration), you can support a mixed configuration of 3D rendering and VRAM sizes for virtual machines in a pool.
- For vDGA (Virtual Dedicated Graphics Acceleration), each virtual machine must be individually configured to share a specific PCI device with the ESXi host and all memory must be reserved. For more information, see "Preparing for vDGA Capabilities," on page 125.

  All ESXi hosts must be version 5.5 or later and must have GPU graphics cards installed.

  Note Some Intel vDGA cards require a certain vSphere 6 version. See the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.
- For AMD Multiuser GPU using vDGA, each virtual machine must be individually configured to share a specific PCI device with the ESXi host and all memory must be reserved. This feature allows a PCI device to appear to be multiple separate physical PCI devices so that the GPU can be shared between 2 to 15 users. For more information, see "Preparing to Use the Capabilities of AMD Multiuser GPU Using vDGA," on page 126.

  All ESXi hosts must be version 6.0 or later and must have GPU graphics cards installed.

You might also choose this option if you want to explicitly manage graphics settings of clones and linked clones by having the clones inherit settings from the parent virtual machine.

When to Choose the NVIDIA GRID vGPU Option

With the **NVIDIA GRID vGPU** option, you can achieve a higher consolidation ratio of virtual machines on an NVIDIA GRID vGPU-enabled ESXi host than is possible by using vDGA, while maintaining the same performance level. As with vDGA (Dedicated Virtual Graphics), the ESXi and virtual machine also use GPU pass-through for NVIDIA GRID vGPU.

Note To improve virtual machine consolidation ratios, you can set the ESXi host to use consolidation mode. Edit the `/etc/vmware/config` file on the ESXi host and add the following entry:

```
vGPU.consolidation = "true"
```

By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is called performance mode. If you would rather have the ESXi host assign virtual machines to the same physical GPU until the maximum number of virtual machines is reached before placing virtual machines on the next physical GPU, you can use consolidation mode.

Because a GPU does not need to be dedicated to one specific virtual machine, with the **NVIDIA GRID vGPU** option, you can create and configure a parent virtual machine or virtual machine template to be NVIDIA GRID vGPU-enabled and then create a desktop pool of virtual machines that can share the same physical GPU.

If all GPU resources on an ESXi host are being used by other virtual machines, when the next user tries to log in to a desktop, View can move the virtual machine to another NVIDIA GRID vGPU-enabled ESXi server in the cluster and then power on the virtual machine. All ESXi hosts must be version 6.0 or later and must have GPU graphics cards installed.

For more information, see "Preparing for NVIDIA GRID vGPU Capabilities," on page 125.

When to Choose the Software Option

Select the **Software** option if you have ESXi 5.0 hosts only, or if ESXi 5.1 or later hosts do not have GPU graphics cards, or if your users only run applications such as AERO and Microsoft Office, which do not require hardware graphics acceleration.

Configuring Desktop Settings to Manage GPU Resources

You can configure other desktop settings to ensure that GPU resources are not wasted when users are not actively using them.

For floating pools, set a session timeout so that GPU resources are freed up for other users when a user is not using the desktop.

For dedicated pools, you can configure the **Automatically logoff after disconnect** setting to **Immediately** and a **Suspend** power policy if these settings are appropriate for your users. For example, do not use these settings for a pool of researchers who execute long-running simulations. Note that the **Suspend** power policy is not available if you use the **NVIDIA GRID vGPU** option.

Preparing for vDGA Capabilities

Virtual Dedicated Graphics Acceleration (vDGA) provides direct pass-through to a physical GPU, providing a user with unrestricted, dedicated access to a single vGPU. Before you attempt to create a desktop pool that has vDGA capabilities, you must perform certain configuration tasks on the virtual machines and ESXi hosts.

This overview is an outline of tasks you must perform in vSphere before you can create or configure desktop pools in View Administrator. For complete information and detailed procedures, see the VMware white paper about graphics acceleration.

Note Some Intel vDGA cards require a certain vSphere 6 version. See the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php. Also, for Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

1 Install the graphics card on the ESXi host.

2 Install the GPU vSphere Installation Bundle (VIB).

3 Verify that VT-d or AMD IOMMU is enabled on the ESXi host.

4 Add a PCI device to the virtual machine and select the appropriate PCI device to enable GPU pass-through on the virtual machine.

5 Reserve all memory when creating the virtual machine.

6 Configure virtual machine video card 3D capabilities.

7 Obtain the GPU drivers from the GPU vendor and install the GPU device drivers in the guest operating system of the virtual machine.

8 Install VMware Tools and Horizon Agent in the guest operating system and reboot.

After you perform these tasks, you must add the virtual machine to a manual desktop pool so that you can access the guest operating system using PCoIP or VMware Blast Extreme. In a PCoIP or VMware Blast session, you can then activate the NVIDIA, AMD, or Intel display adapter in the guest operating system.

Preparing for NVIDIA GRID vGPU Capabilities

NVIDIA GRID vGPU provides direct access to the physical GPU on an ESXi host—so multiple users can share a single GPU—using native graphics card drivers. Before you attempt to create a desktop pool that has NVIDIA GRID vGPU capabilities, you must perform certain configuration tasks on the virtual machines and ESXi hosts.

This overview is an outline of tasks you must perform in vSphere before you can create or configure desktop pools in View Administrator. For complete information and detailed procedures, see the NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1.

1 Install the graphics card on the ESXi host.

2 Install the GPU vSphere Installation Bundle (VIB).

3 Verify that VT-d or AMD IOMMU is enabled on the ESXi host.

4 Enable GPU device pass-through on the ESXi host.

5 Add a shared PCI device to the virtual machine and select the appropriate PCI device to enable GPU pass-through on the virtual machine.

  After you add a shared PCI device, you see a list of all supported graphics profile types that are available from the GPU card on the ESXi host.

6 Reserve all memory when creating the virtual machine.

7 Configure virtual machine video card 3D capabilities.

8 Obtain the GPU drivers from the GPU vendor and install the GPU device drivers in the guest operating system of the virtual machine.

9 Install VMware Tools and Horizon Agent in the guest operating system and reboot.

After you perform these tasks, you must add the virtual machine to a manual pool View desktop pool so that you can access the guest operating system using PCoIP. In a PCoIP session, you can then activate the NVIDIA display adapter in the guest operating system.

At this point, you can configure the virtual machine to be a template or take a snapshot of the virtual machine for use as a base image in a View Composer linked-clone pool. (You must power off the virtual machine before taking the snapshot.) When you use the Add Desktop Pool wizard, after you select the **NVIDIA GRID vGPU** option for **3D Renderer**, only NVIDIA GRID vGPU-enabled ESXi hosts and NVIDIA GRID vGPU-enabled virtual machine templates and snapshots appear for selection in the wizard.

Preparing to Use the Capabilities of AMD Multiuser GPU Using vDGA

AMD Multiuser GPU using vDGA provides direct pass-through to a physical GPU, providing a user with unrestricted, dedicated access to a single GPU. Before you attempt to create a desktop pool that has capabilities to use AMD Multiuser GPU using vDGA, you must perform certain configuration tasks on the virtual machines and ESXi hosts.

This overview is an outline of tasks you must perform in vSphere before you can create or configure desktop pools in View Administrator. For information about enabling GPU device pass-through and adding a PCI device to a virtual machine, see the VMware white paper about graphics acceleration.

1 Install the graphics card on the ESXi host.

2 Install the GPU vSphere Installation Bundle (VIB).

3 Verify that VT-d or AMD IOMMU is enabled on the ESXi host.

4 Use the `esxcfg-module` command to configure the graphics card for SR-IOV (Single Root I/O Virtualization) .

  See "Configuring AMD Multiuser GPU Using vDGA," on page 127.

5 Reboot the ESXi host.

6 Add a PCI device to the virtual machine and select the appropriate PCI device to enable GPU pass-through on the virtual machine.

7 Reserve all memory when creating the virtual machine.

8 Configure virtual machine video card 3D capabilities.

9 Obtain the GPU drivers from the GPU vendor and install the GPU device drivers in the guest operating system of the virtual machine.

10 Install VMware Tools and Horizon Agent in the guest operating system and reboot.

After you perform these tasks, you must add the virtual machine to a manual desktop pool so that you can access the guest operating system using PCoIP or VMware Blast Extreme. If you attempt to access the virtual machine using a vSphere, the display will show a black screen.

Configuring AMD Multiuser GPU Using vDGA

You use the `esxcfg-module` command-line command to configure such parameters as the number of users who can share the GPU, the amount of frame buffer allocated to each user, and some performance control.

Syntax

```
esxcfg-module -s "adapter1_conf=bus#,device#,function#,number_of_VFs,FB_size,time_slice,mode"
amdgpuv
```

Usage Notes

The `vicfg-module` command supports setting and retrieving VMkernel module options on an ESXi host. For general reference information about this command, go to http://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.ref.doc/vicfg-module.html.

Required Flags

You must specify several flags when configuring AMD Multiuser GPU Using vDGA. If the command does not include all the required flags, no error message is provided, but the configuration defaults to a simple 4 SR-IOV device configuration.

Table 9-14. Flags for Configuring AMD SR-IOV

Flag	Description
bus#	Bus number in decimal format.

device#	PCIe device ID for the supported AMD card, in decimal format. To see a list, use the command `lspci | grep -i display`.
	For example, for a system that has two AMD GPU cards, you might see the following output when you run this command:
	`[root@host:~] lspci | grep -i display`
	`0000:04:00.0 Display controller:`
	`0000:82:00.0 Display controller:`
	In this example, the PCIe device IDs are 04 and 82. Note that these IDs are listed in hexadecimal format and must be converted to decimal format for use in the `vicfg-module` command .
	AMD S7150 cards support only a single GPU per card, and so the device ID and function ID are 0 for these cards.

function#	Function number in decimal format.
number_of_VFs	Number of VFs (virtual functions), from 2 to 15. This number represents the number users who will share the GPU.
FB_size	Amount of fame buffer memory, in MB, allocated to each VF. To determine the size, take the overall amount of video memory on the card and divide that amount by the number of VFs. Then round that number to the nearest number that is a multiple of 8. For example, for an AMD S7150 card, which has 8000 MB, you could use the following settings; ■ For 2 VFs, use 4096. ■ For 4 VFs, use 2048. ■ For 8 VFs, use 1024. ■ For 15 VFs, use 544.
time_slice	Interval between VF switches, in microseconds. This setting adjusts the delay in queuing and processing commands between the SR-IOV devices. Use a value between 3000 and 40000. Adjust this value if you see significant stuttering when multiple SR-IOV desktops are active.
mode	Following are the valid values: 0 = reclaimed performance; 1 = fixed percentage performance.

IMPORTANT After you run the `esxcfg-module` command, you must reboot the ESXi host for the settings to take effect.

Examples

1 For a single AMD S7150 card on PCI ID 4 shared between 8 users:

```
esxcfg-module -s "adapter1_conf=4,0,0,8,1024,4000" amdgpuv
```

2 For a single server with two AMD S7150 cards on PCI ID 4 and PCI ID 82 shared between 4 power users:

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,2,4096,4000" amdgpuv
```

3 For a single server with two AMD S7150 cards, you can set each card with different parameters. For instance if your View environment needs to support 2 power users and 16 task workers:

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,15,544,7000" amdgpuv
```

4 Enable the SR-IOV option on the ESXi host.

Some hosts have SR-IOV as a configurable option in the BIOS.

Examining GPU Resources on an ESXi Host

To better manage the GPU resources that are available on an ESXi host, you can examine the current GPU resource reservation. The ESXi command-line query utility, `gpuvm`, lists the GPUs that are installed on an ESXi host and displays the amount of GPU memory that is reserved for each virtual machine on the host. Note that this GPU memory reservation is not the same as virtual machine VRAM size.

To run the utility, type **`gpuvm`** from a shell prompt on the ESXi host. You can use a console on the host or an SSH connection.

For example, the utility might display the following output:

```
~ # gpuvm
Xserver unix:0, GPU maximum memory 2076672KB
        pid 118561, VM "JB-w7-64-FC3", reserved 131072KB of GPU memory.
        pid 64408, VM "JB-w7-64-FC5", reserved 261120KB of GPU memory.
        GPU memory left 1684480KB.
```

Similarly, you can use the `nvidia-smi` command on the ESXi host to see a list of NVIDIA GRID vGPU-enabled virtual machines, the amount of frame buffer memory consumed, and the slot ID of the physical GPU that the virtual machine is using.

Prevent Access to Horizon 7 Desktops Through RDP

In certain Horizon 7 environments, it is a priority to prohibit access to Horizon 7 desktops through the RDP display protocol. You can prevent users and administrators from using RDP to access Horizon 7 desktops by configuring pool settings and a group policy setting.

By default, while a user is logged in to a Horizon 7 desktop session, you can use RDP to connect to the virtual machine from outside of Horizon 7. The RDP connection terminates the Horizon 7 desktop session, and the user's unsaved data and settings might be lost. The user cannot log in to the desktop until the external RDP connection is closed. To avoid this situation, disable the `AllowDirectRDP` setting.

Note Remote Desktop Services must be started on the virtual machine that you use to create pools and on the virtual machines that are deployed in the pools. Remote Desktop Services are required for Horizon Agent installation, SSO, and other Horizon session-management operations.

Prerequisites

Verify that the Horizon Agent Configuration Administrative Template (ADMX or ADM) file is installed in Active Directory. See "Using Horizon 7 Group Policy Administrative Template Files" in the *Configuring Remote Desktop Features in Horizon 7*.

Note In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

Procedure

1 Select PCoIP as the display protocol that you want Horizon Connection Server to use to communicate with Horizon Client devices.

Option	Description
Create a desktop pool	a In Horizon Administrator, start the Add Desktop Pool wizard. b On the Desktop Pool Settings page, select **VMware Blast** or **PCoIP** as the default display protocol.
Edit an existing desktop pool	a In Horizon Administrator, select the desktop pool and click **Edit**. b On the **Desktop Pool Settings** tab, select **VMware Blast** or **PCoIP** as the default display protocol.

2 For the **Allow users to choose protocol** setting, select **No**.

3 Prevent devices that are not running Horizon Client from connecting directly to Horizon desktops through RDP by disabling the `AllowDirectRDP` group policy setting.

a On your Active Directory server, open the Group Policy Management Console and select **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates (ADM) > VMware Horizon Agent Configuration**.

b Disable the `AllowDirectRDP` setting.

Deploying Large Desktop Pools

When many users require the same desktop image, you can create one large automated pool from a single template or parent virtual machine. By using a single base image and pool name, you can avoid dividing the machines arbitrarily into smaller groups that must be managed separately. This strategy simplifies your deployment and administration tasks.

To support large pools, you can create pools on ESXi clusters that contain up to 32 ESXi hosts. You can also configure a pool to use multiple network labels, making the IP addresses of multiple port groups available for the virtual machines in the pool.

Note The multiple network label feature is not available to instant clones.

Configuring Desktop Pools on Clusters With More Than Eight Hosts

In vSphere 5.1 and later, you can deploy a linked clone desktop pool on a cluster that contains up to 32 ESXi hosts. All ESXi hosts in the cluster must be version 5.1 or later. The hosts can use VMFS or NFS datastores. VMFS datastores must be VMFS5 or later.

In vSphere 5.0, you can deploy linked clones on a cluster that contains more than eight ESXi hosts, but you must store the replica disks on NFS datastores. You can store replica disks on VMFS datastores only with clusters that contain eight or fewer hosts.

In vSphere 5.0, the following rules apply when you configure a linked clone pool on a cluster that contains more than eight hosts:

- If you store replica disks on the same datastores as OS disks, you must store the replica and OS disks on NFS datastores.
- If you store replica disks on separate datastores than OS disks, the replica disks must be stored on NFS datastores. The OS disks can be stored on NFS or VMFS datastores.
- If you store View Composer persistent disks on separate datastores, the persistent disks can be configured on NFS or VMFS datastores.

In vSphere 4.1 and earlier releases, you can deploy desktop pools only with clusters that contain eight or fewer hosts.

Assigning Multiple Network Labels to a Desktop Pool

In View 5.2 and later releases, you can configure an automated desktop pool to use multiple network labels. You can assign multiple network labels to a linked-clone pool or an automated pool that contains full virtual machines.

Note The multiple network label feature is not available to instant clones.

In past releases, virtual machines in the pool inherited the network labels that were used by the NICs on the parent virtual machine or template. A typical parent virtual machine or template contains one NIC and one network label. A network label defines a port group and VLAN. The netmask of one VLAN typically provides a limited range of available IP addresses.

In View 5.2 and later releases, you can assign network labels that are available in vCenter Server for all the ESXi hosts in the cluster where the desktop pool is deployed. By configuring multiple network labels for the pool, you greatly expand the number of IP addresses that can be assigned to the virtual machines in the pool.

You must use View PowerCLI cmdlets to assign multiple network labels to a pool. You cannot perform this task in View Administrator.

For details about using View PowerCLI to perform this task, see "Assign Multiple Network Labels to a Desktop Pool" in the chapter "Using View PowerCLI" in the *View Integration* document.

Entitling Users and Groups 10

You configure entitlements to control which remote desktops and applications your users can access. You can configure the restricted entitlements feature to control desktop access based on the View Connection Server instance that users connect to when they select remote desktops. You can also restrict access to a set of users outside the network from connecting to remote desktops and applications within the network.

In a Cloud Pod Architecture environment, you create global entitlements to entitle users or groups to multiple desktops across multiple pods in a pod federation. When you use global entitlements, you do not need to configure and manage local entitlements for remote desktops. For information about global entitlements and setting up a Cloud Pod Architecture environment, see the *Administering View Cloud Pod Architecture* document.

This chapter includes the following topics:

Add Entitlements to a Desktop or Application Pool

Before users can access remote desktops or applications, they must be entitled to use a desktop or application pool.

Prerequisites

Create a desktop or application pool.

Procedure

1 Select the desktop or application pool.

Option	Action
Add an entitlement for a desktop pool	In View Administrator, select **Catalog > Desktop Pools** and click the name of the desktop pool.
Add an entitlement for an application pool	In View Administrator, select **Catalog > Application Pools** and click the name of the application pool.

2 Select **Add entitlement** from the **Entitlements** drop-down menu.

3 Click **Add**, select one or more search criteria, and click **Find** to find users or groups based on your search criteria.

NOTE Domain local groups are filtered out of search results for mixed-mode domains. You cannot entitle users in domain local groups if your domain is configured in mixed mode.

4 Select the users or groups you want to entitle to the desktops or applications in the pool and click **OK**.

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

Remove Entitlements from a Desktop or Application Pool

You can remove entitlements from a desktop or application pool to prevent specific users or groups from accessing a desktop or application.

Procedure

1 Select the desktop or application pool.

Option	Description
Remove an entitlement for a desktop pool	In View Administrator, select **Catalog > Desktop Pools** and click the name of the desktop pool.
Remove an entitlement for an application pool	In View Administrator, select **Catalog > Application Pools** and click the name of the application pool.

2 Select **Remove entitlement** from the **Entitlements** drop-down menu.

3 Select the user or group whose entitlement you want to remove and click **Remove**.

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

Review Desktop or Application Pool Entitlements

You can review the desktop or application pools to which a user or group is entitled.

Procedure

1 In View Administrator, select **Users and Groups** and click the name of the user or group.

2 Click the **Entitlements** tab and review the desktop or application pools to which the user or group is entitled.

Option	Action
List the desktop pools to which the user or group is entitled	Click **Desktop Pools**.
List the application pools to which the user or group is entitled	Click **Application Pools**.

Restricting Remote Desktop Access

You can configure the restricted entitlements feature to restrict remote desktop access based on the Connection Server instance to which users connect when they select desktops.

With restricted entitlements, you assign one or more tags to a Connection Server instance. Then, when you configure a desktop pool, you select the tags of the Connection Server instances that you want to have access to the desktop pool.

When users log in to a tagged Connection Server instance, they can access only those desktop pools that have at least one matching tag or no tags.

You cannot configure the restricted entitlements feature to restrict access to remote applications.

For information about using tags to restrict access to global entitlements in a Cloud Pod Architecture environment, see the *Administering Cloud Pod Architecture in Horizon 7* document.

- Restricted Entitlement Example on page 133

  This example shows a Horizon deployment that includes two Connection Server instances. The first instance supports internal users. The second instance is paired with a security server and supports external users.

- Tag Matching on page 134

  The restricted entitlements feature uses tag matching to determine whether a Connection Server instance can access a particular desktop pool.

- Considerations and Limitations for Restricted Entitlements on page 135

  Before implementing restricted entitlements, you must be aware of certain considerations and limitations.

- Assign a Tag to a Connection Server Instance on page 135

  When you assign a tag to a Connection Server instance, users who connect to that Connection Server instance can access only those desktop pools that have a matching tag or no tags.

- Assign a Tag to a Desktop Pool on page 135

  When you assign a tag to a desktop pool, only users who connect to a Connection Server instance that has a matching tag can access the desktops in that pool.

Restricted Entitlement Example

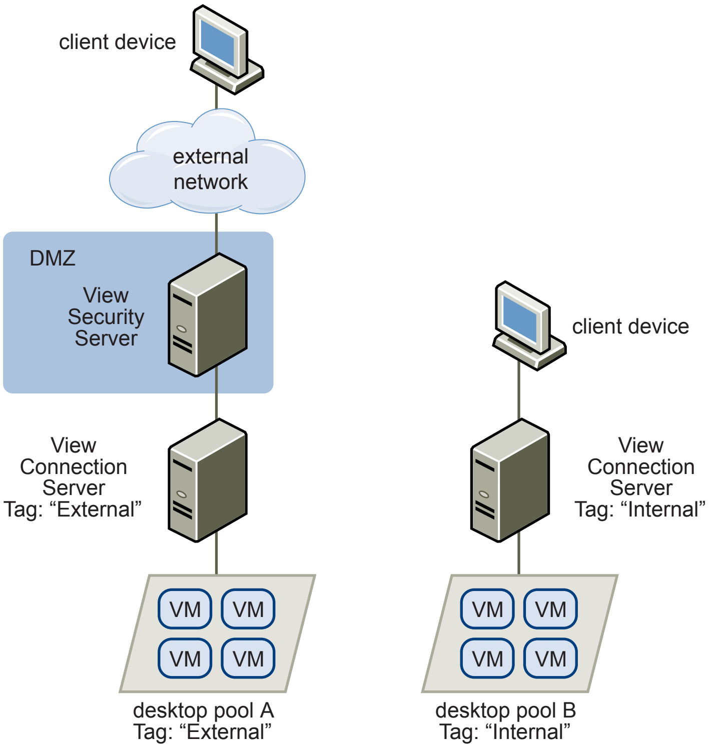
This example shows a Horizon deployment that includes two Connection Server instances. The first instance supports internal users. The second instance is paired with a security server and supports external users.

To prevent external users from accessing certain desktops, you could set up restricted entitlements as follows:

- Assign the tag "Internal" to the Connection Server instance that supports your internal users.
- Assign the tag "External" to the Connection Server instance that is paired with the security server and supports your external users.
- Assign the "Internal" tag to the desktop pools that should be accessible only to internal users.
- Assign the "External" tag to the desktop pools that should be accessible only to external users.

External users cannot see the desktop pools tagged as Internal because they log in through the Connection Server instance that is tagged as External, and internal users cannot see the desktop pools tagged as External because they log in through the Connection Server instance that is tagged as Internal. Figure 10-1 illustrates this configuration.

Figure 10-1. Restricted Entitlement Configuration


client device
external network
DMZ
View Security Server
View Connection Server Tag: “External”
VM
VM
VM
VM
desktop pool A Tag: “External”
client device
View Connection Server Tag: “Internal”
VM
VM
VM
VM
desktop pool B Tag: “Internal”

You can also use restricted entitlements to control desktop access based on the user-authentication method that you configure for a particular Connection Server instance. For example, you can make certain desktop pools available only to users who have authenticated with a smart card.

Tag Matching

The restricted entitlements feature uses tag matching to determine whether a Connection Server instance can access a particular desktop pool.

At the most basic level, tag matching determines that a Connection Server instance that has a specific tag can access a desktop pool that has the same tag.

The absence of tag assignments can also affect whether a Connection Server instance can access a desktop pool. For example, Connection Server instances that do not have any tags can access only desktop pools that also do not have any tags.

Table 10-1 shows how the restricted entitlement feature determines when a Connection Server can access a desktop pool.

Table 10-1. Tag Matching Rules

View Connection Server	Desktop Pool	Access Permitted?
No tags	No tags	Yes
No tags	One or more tags	No
One or more tags	No tags	Yes
One or more tags	One or more tags	Only when tags match

The restricted entitlements feature only enforces tag matching. You must design your network topology to force certain clients to connect through a particular Connection Server instance.

Considerations and Limitations for Restricted Entitlements

Before implementing restricted entitlements, you must be aware of certain considerations and limitations.

- A single Connection Server instance or desktop pool can have multiple tags.
- Multiple Connection Server instances and desktop pools can have the same tag.
- Any Connection Server instance can access a desktop pool that does not have any tags.
- Connection Server instances that do not have any tags can access only desktop pools that also do not have any tags.
- If you use a security server, you must configure restricted entitlements on the Connection Server instance with which the security server is paired. You cannot configure restricted entitlements on a security server.
- You cannot modify or remove a tag from a Connection Server instance if that tag is still assigned to a desktop pool and no other Connection Server instances have a matching tag.
- Restricted entitlements take precedence over other desktop entitlements or assignments. For example, even if a user is assigned to a particular machine, the user cannot access that machine if the tag assigned to the desktop pool does not match the tag assigned to the Connection Server instance to which the user is connected.
- If you intend to provide access to your desktops through VMware Identity Manager and you configure Connection Server restrictions, the VMware Identity Manager app might display desktops to users when those desktops are actually restricted. When a VMware Identity Manager user attempts to log in to a desktop, the desktop does not start if the tag assigned to the desktop pool does not match the tag assigned to the Connection Server instance to which the user is connected.

Assign a Tag to a Connection Server Instance

When you assign a tag to a Connection Server instance, users who connect to that Connection Server instance can access only those desktop pools that have a matching tag or no tags.

Procedure

1. In Horizon Administrator, select **View Configuration > Servers**.
2. Click the **Connection Servers** tab, select the Connection Server instance, and click **Edit**.
3. Type one or more tags in the **Tags** text box.

   Separate multiple tags with a comma or semicolon.
4. Click **OK** to save your changes.

What to do next

Assign the tag to desktop pools. See "Assign a Tag to a Desktop Pool," on page 135.

Assign a Tag to a Desktop Pool

When you assign a tag to a desktop pool, only users who connect to a Connection Server instance that has a matching tag can access the desktops in that pool.

You can assign a tag when you add or edit a desktop pool.

Prerequisites

Assign tags to one or more Connection Server instances.

Procedure

1 In Horizon Administrator, select **Catalog > Desktop Pools**.

2 Select the desktop pool.

Option	Action
Assign a tag to a new pool	Click **Add** to start the Add Desktop Pool wizard and define and identify the pool.
Assign a tag to an existing pool	Select the pool and click **Edit**.

3 Go to the Desktop Pool Settings page.

Option	Action
Pool settings for a new pool	Click **Desktop Pool Settings** in the Add Desktop Pool wizard.
Pool settings for an existing pool	Click the **Desktop Pool Settings** tab.

4 Click **Browse** next to **Connection Server restrictions** and configure the Connection Server instances that can access the desktop pool.

Option	Action
Make the pool accessible to any Connection Server instance	Select **No Restrictions**.
Make the pool accessible only to Connection Server instances that have those tags	Select **Restricted to these tags** and select one or more tags. You can use the check boxes to select multiple tags.

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

Restricting Remote Desktop Access Outside the Network

You can allow access to specific entitled users and groups from an external network while restricting access to other entitled users and groups. All entitled users will have access to desktops and applications from within the internal network. If you choose not to restrict access to specific users from the external network, then all entitled users will have access from the external network.

For security reasons, administrators might need to restrict users and groups outside the network from accessing remote desktops and applications inside the network. When a restricted user accesses the system from an external network, a message stating that the user is not entitled to use the system appears. The user must be inside the internal network to get access to desktop and application pool entitlements.

Restrict Users Outside the Network

You can allow access to the View Connection Server instance from outside the network to users and groups while restricting access for other users and groups.

Prerequisites

- An Access Point appliance, security server, or load balancer must be deployed outside the network as a gateway to the View Connection Server instance to which the user is entitled. For more information about deploying an Access Point appliance, see the *Deploying and Configuring Access Point* document.
- The users who get remote access must be entitled to desktop or application pools.

Procedure

1 In View Administrator, select **Users and Groups**.

2 Click the **Remote Access** tab.

3 Click **Add** and select one or more search criteria, and click **Find** to find users or groups based on your search criteria.

4 To provide remote access for a user or group, select a user or group and click **OK**.

5 To remove a user or group from remote access, select the user or group, click **Delete**, and click **OK**.

Reducing and Managing Storage Requirements 11

Deploying desktops on virtual machines that are managed by vCenter Server provides all the storage efficiencies that were previously available only for virtualized servers. Using instant clones or View Composer linked clones as desktop machines increases the storage savings because all virtual machines in a pool share a virtual disk with a base image.

This chapter includes the following topics:

Managing Storage with vSphere

vSphere lets you virtualize disk volumes and file systems so that you can manage and configure storage without having to consider where the data is physically stored.

Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are widely used storage technologies supported by vSphere to meet different datacenter storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines.

Compatible vSphere 5.0 and 5.1 or Later Features

With vSphere 5.0 or a later release, you can use the following features:

- With the View storage accelerator feature, you can configure ESXi hosts to cache virtual machine disk data.

  Using this content-based read cache (CBRC) can reduce IOPS and improve performance during boot storms, when many machines start up and run anti-virus scans at the same time. Instead of reading the entire OS from the storage system over and over, a host can read common data blocks from cache.

- If remote desktops use the space-efficient disk format available with vSphere 5.1 and later, stale or deleted data within a guest operating system is automatically reclaimed with a wipe and shrink process.

- You can deploy a desktop pool on a cluster that contains up to 32 ESXi hosts, with certain restrictions.

  Replica disks must be stored on VMFS5 or later datastores or NFS datastores. If you store replicas on a VMFS version earlier than VMFS5, a cluster can have at most eight hosts. OS disks and persistent disks can be stored on NFS or VMFS datastores.

Compatible vSphere 5.5 Update 1 or Later Features

With vSphere 5.5 Update 1 or a later release, you can use Virtual SAN, which virtualizes the local physical solid-state disks and hard disk drives available on ESXi hosts into a single datastore shared by all hosts in a cluster. Virtual SAN provides high-performance storage with policy-based management, so that you specify only one datastore when creating a desktop pool, and the various components, such as virtual machine files, replicas, user data, and operating system files, are placed on the appropriate solid-state drive (SSD) disks or direct-attached hard disks (HDDs).

Virtual SAN also lets you manage virtual machine storage and performance by using storage policy profiles. If the policy becomes noncompliant because of a host, disk, or network failure, or workload changes, Virtual SAN reconfigures the data of the affected virtual machines and optimizes the use of resources across the cluster. You can deploy a desktop pool on a cluster that contains up to 20 ESXi hosts.

Important The Virtual SAN feature available with vSphere 6.0 and later releases contains many performance improvements over the feature that was available with vSphere 5.5 Update 1. With vSphere 6.0 this feature also has broader HCL (hardware compatibility) support. For more information about Virtual SAN in vSphere 6 or later, see the *Administering VMware Virtual SAN* document.

Note Virtual SAN is compatible with the View storage accelerator feature but not with the space-efficient disk format feature, which reclaims disk space by wiping and shrinking disks.

Compatible vSphere 6.0 or Later Features

With vSphere 6.0 or a later release, you can use Virtual Volumes (VVols). This feature maps virtual disks and their derivatives, clones, snapshots, and replicas, directly to objects, called virtual volumes, on a storage system. This mapping allows vSphere to offload intensive storage operations such as snapshoting, cloning, and replication to the storage system.

Virtual Volumes also lets you manage virtual machine storage and performance by using storage policy profiles in vSphere. These storage policy profiles dictate storage services on a per-virtual-machine basis. This type of granular provisioning increases capacity utilization. You can deploy a desktop pool on a cluster that contains up to 32 ESXi hosts.

Note Virtual Volumes is compatible with the View storage accelerator feature but not with the space-efficient disk format feature, which reclaims disk space by wiping and shrinking disks.

Note Instant clones do not support Virtual Volumes.

Using Virtual SAN for High-Performance Storage and Policy-Based Management

VMware Virtual SAN is a software-defined storage tier, available with vSphere 5.5 Update 1 or a later release, that virtualizes the local physical storage disks available on a cluster of vSphere hosts. You specify only one datastore when creating an automated desktop pool or an automated farm, and the various components, such as virtual machine files, replicas, user data, and operating system files, are placed on the appropriate solid-state drive (SSD) disks or direct-attached hard disks (HDDs).

Virtual SAN implements a policy-based approach to storage management. When you use Virtual SAN, View defines virtual machine storage requirements, such as capacity, performance, and availability, in the form of default storage policy profiles, which you can modify. Storage is provisioned and automatically configured according to the assigned policies. You can use Virtual SAN for linked-clone desktop pools, instant-clone desktop pools, full-clone desktop pools, or an automated farm.

Each virtual machine maintains its policy regardless of its physical location in the cluster. If the policy becomes noncompliant because of a host, disk, or network failure, or workload changes, Virtual SAN reconfigures the data of the affected virtual machines and load-balances to meet the policies of each virtual machine.

While supporting VMware features that require shared storage, such as HA, vMotion, and DRS, Virtual SAN eliminates the need for an external shared storage infrastructure and simplifies storage configuration and virtual machine provisioning activities.

Important The Virtual SAN feature available with vSphere 6.0 and later releases contains many performance improvements over the feature that was available with vSphere 5.5 Update 1. With vSphere 6.0 this feature also has broader HCL (hardware compatibility) support. Also, VMware Virtual SAN 6.0 supports an all-flash architecture that uses flash-based devices for both caching and persistent storage.

Virtual SAN Workflow in View

1. Use vCenter Server 5.5 Update 1 or a later release to enable Virtual SAN. For more information about Virtual SAN in vSphere 5.5 Update 1, see the *vSphere Storage* document. For more information about Virtual SAN in vSphere 6 or later, see the *Administering VMware Virtual SAN* document.

2. When creating an automated desktop pool or an automated farm in View Administrator, under **Storage Policy Management**, select **Use VMware Virtual SAN**, and select the Virtual SAN datastore to use.

   After you select **Use VMware Virtual SAN**, only Virtual SAN datastores are displayed.

   Default storage policy profiles are created according to the options you choose. For example, if you create a linked-clone, floating desktop pool, a replica disk profile and an operating system disk profile are automatically created. If you create a linked-clone, persistent desktop pool, a replica disk profile and a persistent disk profile are created. For an automated farm, a replica disk profile is created. For both types of desktop pools and automated farms, a profile is created for virtual machine files.

3. To move existing View Composer desktop pools from another type of datastore to a Virtual SAN datastore, in View Administrator, edit the pool to deselect the old datastore and select the Virtual SAN datastore instead, and use the Rebalance command. This operation is not possible for automated farms because you cannot rebalance an automated farm .

4. (Optional) Use vCenter Server to modify the parameters of the storage policy profiles, which include things like the number of failures to tolerate and the amount of SSD read cache to reserve.

   The names of the policies are OS_DISK (for operating system files), PERSISTENT_DISK (for user data files), REPLICA_DISK (for replicas), and VM_HOME (for virtual machine files such as `.vmx` and `.vmsn` files). Changes to the policy are propagated to newly created virtual machines and to all existing virtual machines in the desktop pool or the automated farm.

5. Use vCenter Server to monitor the Virtual SAN cluster and the disks that participate in the datastore. For more information, see the *vSphere Storage* document and the *vSphere Monitoring and Performance* documentation. For vSphere 6 or later, see the *Administering VMware Virtual SAN* document.

6. (Optional) For View Composer linked-clone desktop pools, use the Refresh and Recompose commands as you normally would. For automated farms, only the Recompose command is supported, regardless of the type of datastore.

Requirements and Limitations

The Virtual SAN feature has the following limitations when used in a View deployment:

- This release does not support using the View space-efficient disk format feature, which reclaims disk space by wiping and shrinking disks.
- Virtual SAN does not support the View Composer Array Integration (VCAI) feature because Virtual SAN does not use NAS devices.

Note Virtual SAN is compatible with the View Storage Accelerator feature. Virtual SAN provides a caching layer on SSD disks, and the View Storage Accelerator feature provides a content-based cache that reduces IOPS and improves performance during boot storms.

The Virtual SAN feature has the following requirements:

- vSphere 5.5 Update 1 or a later release.
- Appropriate hardware. For example, VMware recommends a 10GB NIC and at least one SSD and one HDD for each capacity-contributing node. For specifics, see the VMware Compatibility Guide.
- A cluster of at least three ESXi hosts. You need enough ESXi hosts to accommodate your setup even if you use two ESXi hosts with a Virtual SAN stretched cluster. For more information, see the *vSphere Configuration Maximums* document.
- SSD capacity that is at least 10 percent of HDD capacity.
- Enough HDDs to accommodate your setup. Do not exceed more than 75% utilization on a magnetic disk.

For more information about Virtual SAN requirements, see "Working with Virtual SAN" in the *vSphere 5.5 Update 1 Storage* document. For vSphere 6 or later, see the *Administering VMware Virtual SAN* document. For guidance on sizing and designing the key components of View virtual desktop infrastructures for VMware Virtual SAN, see the white paper at http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf.

Default Storage Policy Profiles for Virtual SAN Datastores

When you use Virtual SAN, View defines virtual machine storage requirements, such as capacity, performance, and availability, in the form of default storage policy profiles, which you can modify. Storage is provisioned and automatically configured according to the assigned policies.

The default policies that are created during desktop pool creation depend on the type of pool you create. The names of the policies are OS_DISK (for operating system files), PERSISTENT_DISK (for user data files), REPLICA_DISK (for replicas), and VM_HOME (for virtual machine files such as `.vmx` and `.vmsn` files). For example, a REPLICA_DISK policy is created only for linked-clone pools. Changes to the policy are propagated to newly created virtual machines and to all existing virtual machines in the desktop pool.

Virtual SAN offers a storage policy framework so that you can control the behavior of various virtual machine objects that reside on the Virtual SAN datastore. An example of an object in Virtual SAN is a virtual disk (VMDK) file, and there are four characteristics of each object that are controlled through policy:

- **Stripes**: Number of stripes of data. The number of disk stripes affects how many magnetic disks you have (HDDs).
- **Resiliency**: Number of failures to tolerate. The number of host failures to tolerate depends, of course, on the number of hosts you have.
- **Storage Provisioning**: Thick or Thin.
- **Cache Reservation**: Read-cache reservation.

The stripes and cache reservation settings are used to control performance. The resiliency setting controls availability. The storage provisioning setting control capacity. These settings, taken together, affect how many vSphere hosts and magnetic disks are required.

For example, if you set the number of disk stripes per object to 2, Virtual SAN will stripe the object across at least 2 HDDs. In conjunction with this setting, if you set the number of host failures to tolerate to 1, Virtual SAN will create an additional copy for resiliency and therefore require 4 HDDs. Additionally, setting the number of host failures to tolerate to 1 requires a minimum of 3 ESXi hosts, 2 for resiliency and the third to break the tie in case of partitioning.

NOTE If you inadvertently attempt to use settings that contradict each other, when you attempt to apply the settings, the operation will fail, and an error message will tell you, for example, that you do not have enough hosts.

There is no requirement for any user action associated with these default policies. Policies are created for linked-clone desktop pools, full-clone desktop pools, and automated farms.

You can use either the vSphere Command-Line Interface (`esxcli`) or the vSphere Web Client to change the default storage policy profiles. Each virtual machine maintains its policy regardless of its physical location in the cluster. If the policy becomes noncompliant because of a host, disk, or network failure, or workload changes, Virtual SAN reconfigures the data of the affected virtual machines and load-balances to meet the policies of each virtual machine.

Using Virtual Volumes for Virtual-Machine-Centric Storage and Policy-Based Management

With Virtual Volumes (VVols), available with vSphere 6.0 or a later release, an individual virtual machine, not the datastore, becomes a unit of storage management. The storage hardware gains control over virtual disk content, layout, and management.

With Virtual Volumes, abstract storage containers replace traditional storage volumes based on LUNs or NFS shares. Virtual Volumes maps virtual disks and their derivatives, clones, snapshots, and replicas, directly to objects, called virtual volumes, on a storage system. With this mapping, vSphere can offload intensive storage operations such as snapshoting, cloning, and replication to the storage system. The result, for example, is that a cloning operation that previously took an hour might now take a few minutes using Virtual Volumes.

Important One of the key benefits of Virtual Volumes is the ability to use Software Policy-Based Management (SPBM). However, for this release, View does not create the default granular storage policies that Virtual SAN creates. Instead, you can set a global default storage policy in vCenter Server that applies to all Virtual Volume datastores.

Virtual Volumes has the following benefits:

- Virtual Volumes supports offloading a number of operations to storage hardware. These operations include snapshotting, cloning, and Storage DRS.
- With Virtual Volumes, you can use advanced storage services that include replication, encryption, deduplication, and compression on individual virtual disks.
- Virtual Volumes supports such vSphere features as vMotion, Storage vMotion, snapshots, linked clones, Flash Read Cache, and DRS.
- You can use Virtual Volumes with storage arrays that support vSphere APIs for Array Integration (VAAI).

Requirements and Limitations

The Virtual Volumes feature has the following limitations when used in a View deployment:

- This release does not support using the View space-efficient disk format feature, which reclaims disk space by wiping and shrinking disks.
- Virtual Volumes does not support using View Composer Array Integration (VCAI).
- Virtual Volumes datastores are not supported for instant clone desktop pools.

Note Virtual Volumes is compatible with the View Storage Accelerator feature. Virtual SAN provides a caching layer on SSD disks, and the View Storage Accelerator feature provides a content-based cache that reduces IOPS and improves performance during boot storms.

The Virtual Volumes feature has the following requirements:

- vSphere 6.0 or a later release.
- Appropriate hardware. Certain storage vendors are responsible for supplying storage providers that can integrate with vSphere and provide support for Virtual Volumes. Every storage provider must be certified by VMware and properly deployed.
- All virtual disks that you provision on a virtual datastore must be an even multiple of 1 MB.

Virtual Volumes is a vSphere 6.0 feature. For more information about the requirements, functionality, background, and setup requirements, see the topics about Virtual Volumes in the *vSphere Storage* document.

Reducing Storage Requirements with Instant Clones

The instant clones feature leverages vSphere vmFork technology (available with vSphere 6.0U1 and later) to quiesce a running base image, or parent virtual machine, and hot-clone it to create a pool of up to 2,000 instant clones.

Not only do instant clones share the virtual disks with the parent virtual machine at the time of creation, instant clones also share the memory of the parent. Each instant clone acts like an independent desktop, with a unique host name and IP address, yet the instant clone requires significantly less storage. Instant clones reduce the required storage capacity by 50 to 90 percent. The overall memory requirement is also reduced at clone creation time.

Replica and Instant Clones on the Same Datastore

When you create an instant clone desktop pool, a full clone is first made from the master virtual machine. The full clone, or replica, and the clones linked to it can be placed on the same data store, or LUN (logical unit number).

Replica and Instant Clones on Different Datastores

Alternatively, you can place instant clone replicas and instant clones on separate datastores with different performance characteristics. For example, you can store the replica virtual machines on a solid-state drive (SSD). Solid-state drives have low storage capacity and high read performance, typically supporting tens of thousands of I/Os per second (IOPS).

You can store instant clones on traditional, spinning media-backed datastores. These disks provide lower performance, but are less expensive and provide higher storage capacity, which makes them suited for storing the many instant clones in a large pool. Tiered storage configurations can be used to cost-effectively handle intensive I/O scenarios such as simultaneous running scheduled antivirus scans.

If you use Virtual SAN datastores, you cannot manually select different datastores for replicas and instant clones. Because Virtual SAN automatically places objects on the appropriate type of disk and caches all I/O operations, there is no need to use replica tiering for Virtual SAN data stores. Instant clone pools are supported on Virtual SAN data stores. Instant clone pools are not supported on ordinary local storage disks.

Differences between Instant Clones and View Composer Linked Clones

Since instant clones can be created significantly faster than linked clones, the following features of linked clones are no longer needed when you provision a pool of instant clones:

- Instant clone pools do not support configuration of a separate, disposable virtual disk for storing the guest operating system's paging and temp files. Each time a user logs out of an instant clone desktop, View automatically deletes the clone and provisions and powers on another instant clone based on the latest OS image available for the pool. Any guest operating systems paging and temp files are automatically deleted during the logoff operation.
- Instant clone pools do not support the creation of a separate persistent virtual disk for each virtual desktop. Instead, you can store the end user's Windows profile and application data on App Volumes' user writable disks. An end user's user writable disk is attached to an instant clone desktop when the end user logs in. In addition, user writable disks can be used to persist user-installed applications.
- Due to short-lived nature of instant clone desktops, the space-efficient disk format (SE sparse), with its wipe and shrink process, is not needed.

Reducing Storage Requirements with View Composer

Because View Composer creates desktop images that share virtual disks with a base image, you can reduce the required storage capacity by 50 to 90 percent.

View Composer uses a base image, or parent virtual machine, and creates a pool of up to 2,000 linked-clone virtual machines. Each linked clone acts like an independent desktop, with a unique host name and IP address, yet the linked clone requires significantly less storage.

Replica and Linked Clones on the Same Datastore

When you create a linked-clone desktop pool or farm of Microsoft RDS hosts, a full clone is first made from the parent virtual machine. The full clone, or replica, and the clones linked to it can be placed on the same data store, or LUN (logical unit number). If necessary, you can use the rebalance feature to move the replica and linked-clone desktop pools from one LUN to another or to move linked-clone desktop pools to a Virtual SAN datastore or from a Virtual SAN datastore to a LUN.

Replica and Linked Clones on Different Datastores

Alternatively, you can place View Composer replicas and linked clones on separate datastores with different performance characteristics. For example, you can store the replica virtual machines on a solid-state drive (SSD). Solid-state drives have low storage capacity and high read performance, typically supporting tens of thousands of I/Os per second (IOPS). You can store linked clones on traditional, spinning media-backed datastores. These disks provide lower performance, but are less expensive and provide higher storage capacity, which makes them suited for storing the many linked clones in a large pool. Tiered storage configurations can be used to cost-effectively handle intensive I/O scenarios such as simultaneous rebooting of many virtual machines or running scheduled antivirus scans.

For more information, see the best-practices guide called *Storage Considerations for VMware View.*

If you use Virtual SAN datastores or Virtual Volumes datastores, you cannot manually select different datastores for replicas and linked clones. Because the Virtual SAN and Virtual Volumes features automatically place objects on the appropriate type of disk and cache of all I/O operations, there is no need to use replica tiering for Virtual SAN and Virtual Volumes datastores.

Disposable Disks for Paging and Temp Files

When you create a linked-clone pool or farm, you can also optionally configure a separate, disposable virtual disk to store the guest operating system's paging and temp files that are generated during user sessions. When the virtual machine is powered off, the disposable disk is deleted. Using disposable disks can save storage space by slowing the growth of linked clones and reducing the space used by powered off virtual machines.

Persistent Disks for Dedicated Desktops

When you create dedicated-assignment desktop pools, View Composer can also optionally create a separate persistent virtual disk for each virtual desktop. The end user's Windows profile and application data are saved on the persistent disk. When a linked clone is refreshed, recomposed, or rebalanced, the contents of the persistent virtual disk are preserved. VMware recommends that you keep View Composer persistent disks on a separate datastore. You can then back up the whole LUN that holds persistent disks.

Storage Sizing for Instant-Clone and View Composer Linked-Clone Desktop Pools

View provides high-level guidelines that can help you determine how much storage an instant-clone or linked-clone desktop pool requires. A table in the Add Desktop Pool wizard shows a general estimate of the desktop pool's storage requirements.

The storage-sizing table also displays the free space on the datastores that you select for storing OS disks, View Composer persistent disks (for View Composer linked clones only), and replicas. You can decide which datastores to use by comparing the actual free space with the estimated requirements for the desktop pool.

The formulas that View uses can only provide a general estimate of storage use. The clones' actual storage growth depends on many factors:

- Amount of memory assigned to the parent virtual machine
- Frequency of refresh operations (for View Composer linked clones only)
- Size of the guest operating system's paging file
- Whether you redirect paging and temp files to a separate disk (for View Composer linked clones only)
- Whether you configure separate View Composer persistent disks (for View Composer linked clones only)
- Workload on the desktop machines, determined primarily by the types of applications that users run in the guest operating system

Note In a deployment that includes hundreds or thousands of clones, configure your desktop pool so that particular sets of datastores are dedicated to particular ESXi clusters. Do not configure pools randomly across all the datastores so that most or all ESXi hosts must access most or all LUNs.

When too many ESXi hosts attempt to write to the OS disks on a particular LUN, contention problems can occur, degrading performance and interfering with scalability. For more information about datastore planning in large deployments, see the *View Architecture Planning* document.

Sizing Guidelines for Instant-Clone and Linked-Clone Pools

When you create or edit an instant-clone or linked-clone desktop pool, the Select Linked (or Instant) Clone Datastores page displays a table that provides storage-sizing guidelines. The table can help you to decide which datastores to select for the linked-clone disks. The guidelines calculate space needed for new linked clones.

Sizing Table for OS Disks and Persistent Disks

Table 11-1 shows an example of storage-sizing recommendations that might be displayed for a pool of 10 virtual machines if the parent virtual machine has 1GB of memory and a 10GB replica. In this example, different datastores are selected for OS disks and View Composer persistent disks.

Note The persistent disk information is for View Composer linked clones only. Instant clones do not support persistent disks.

Table 11-1. Example Sizing Table for OS and Persistent Disks

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	40.00	80.00	130.00
Persistent disks	28.56	4.00	10.00	20.00

The **Selected Free Space** column shows the total available space on all of the datastores that you selected for a disk type such as OS disks.

The **Min Recommended** column shows the minimum amount of recommended storage for a pool.

The **50% Utilization** column shows the recommended storage when the disks grow to 50% of the parent virtual machine.

The **Max Recommended** column shows the recommended storage when the disks approach the full size of the parent virtual machine.

If you store OS disks and persistent disks on the same datastore, View calculates the storage requirements of both disk types. The **Data Type** is shown as **Linked clones** or **Instant clones** instead of a particular disk type.

If you store View Composer replicas on a separate datastore, the table also shows storage recommendations for the replicas and adjusts the recommendations for OS disks.

Sizing Guidelines for View Composer Linked Clones

The table provides general guidelines. Your storage calculations must account for additional factors that can affect actual storage growth in the clones.

For OS disks, your sizing estimates depend on how frequently you refresh and recompose the pool.

If you refresh your linked-clone pool between once a day and once a week, make sure that the **Selected Free Space** can accommodate storage use between the **Min Recommended** and **50% Utilization** estimates.

If you rarely refresh or recompose the pool, the linked-clone disks continue to grow. Make sure that the **Selected Free Space** can accommodate storage use between the **50 % Utilization** and **Max Recommended** estimates.

For persistent disks, your sizing estimates depend on the amount of Windows profile data that users generate on their desktops. Refresh and recompose operations do not affect persistent disks.

Sizing Guidelines When You Edit an Existing Desktop Pool

View estimates the storage space that is needed for new clones. When you create a desktop pool, the sizing guidelines encompass the entire pool. When you edit an existing desktop pool, the guidelines encompass only the new clones that you add to the pool.

For example, if you add 100 clones to a desktop pool and select a new datastore, View estimates space requirements for the 100 new clones.

If you select a new datastore but keep the desktop pool the same size, or reduce the number of clones, the sizing guidelines show as 0. The values of 0 reflect that no new clones must be created on the selected datastore. Space requirements for the existing clones are already accounted for.

How View Calculates the Minimum Sizing Recommendations

To arrive at a minimum recommendation for OS disks, View estimates that each clone consumes twice its memory size when it is first created and started up. If no memory is reserved for a clone, an ESXi swap file is created for a clone as soon as it is powered on. The size of the guest operating system's paging file also affects the growth of a clone's OS disk.

In the minimum recommendation for OS disks, View also includes space for two replicas on each datastore. View Composer creates one replica when a pool is created. When the pool is recomposed for the first time, View Composer creates a second replica on the datastore, anchors the clones to the new replica, and deletes the first replica if no other clones are using original snapshot. The datastore must have the capacity to store two replicas during the recompose operation.

By default, replicas use vSphere thin provisioning, but to keep the guidelines simple, View accounts for two replicas that use the same space as the parent virtual machine.

To arrive at a minimum recommendation for persistent disks, View calculates 20% of the disk size that you specify on the **View Composer Disks** page of the Add Desktop Pool wizard.

Note The calculations for persistent disks are based on static threshold values, in gigabytes. For example, if you specify a persistent disk size of any value between 1024MB and 2047MB, View calculates the persistent disk size as 1GB. If you specify a disk size of 2048MB, View calculates the disk size as 2GB.

To arrive at a recommendation for storing replicas on a separate datastore, View allows space for two replicas on the datastore. The same value is calculated for minimum and maximum usage.

For details, see "Sizing Formulas for Instant-Clone and Linked-Clone Pools," on page 149.

Sizing Guidelines and Storage Overcommit for View Composer Linked Clones

Note Instant clones do not support storage overcommit.

After you estimate storage requirements, select datastores, and deploy the pool, View provisions linked-clone virtual machines on different datastores based on the free space and the existing clones on each datastore.

Based on the storage-overcommit option that you select on the Select Linked Clone Datastores page in the Add Desktop Pool wizard, View stops provisioning new clones and reserves free space for the existing clones. This behavior ensures that a growth buffer exists for each machine in the datastore.

If you select an aggressive storage-overcommit level, the estimated storage requirements might exceed the capacity shown in the **Selected Free Space** column. The storage-overcommit level affects how many virtual machines that View actually creates on a datastore.

For details, see "Set the Storage Overcommit Level for Linked-Clone Virtual Machines," on page 152.

Sizing Formulas for Instant-Clone and Linked-Clone Pools

Storage-sizing formulas can help you estimate how much disk space is required on the datastores that you select for OS disks, View Composer persistent disks, and replicas.

Note The persistent disk information is for View Composer linked clones only. Instant clones do not support persistent disks.

Storage Sizing Formulas

Table 11-2 shows the formulas that calculate the estimated sizes of the disks when you create a pool and as the clones grow over time. These formulas include the space for replica disks that are stored with the clones on the datastore.

If you edit an existing pool or store replicas on a separate datastore, View uses a different sizing formula. See "Sizing Formulas for Creating Clones When You Edit a Pool or Store Replicas on a Separate Datastore," on page 150.

Table 11-2. Storage Sizing Formulas for Clone Disks on Selected Datastores

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	Free space on the selected datastores	Number of VMs * (2 * memory of VM) + (2 * replica disk)	Number of VMs * (50% of replica disk + memory of VM) + (2 * replica disk)	Number of VMs * (100% of replica disk + memory of VM) + (2 * replica disk)
Persistent disks	Free space on the selected datastores	Number of VMs * 20% of persistent disk	Number of VMs * 50% of persistent disk	Number of VMs * 100% of persistent disk

Example of a Storage Sizing Estimate

In this example, the parent virtual machine is configured with 1GB of memory. The parent virtual machine's disk size is 10GB. A pool is created with 10 machines. Persistent disks are configured as 2048MB in size.

The OS disks are configured on a datastore that currently has 184.23GB of available space. The persistent disks are configured on a different datastore with 28.56GB of available space.

Table 11-3 shows how the sizing formulas calculate estimated storage requirements for the sample desktop pool.

Table 11-3. Example of a Sizing Estimate for Clone Disks Deployed on Selected Datastores

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	10 * (2*1GB) + (2*10GB) = 40.00	10 * (50% of 10GB + 1GB) + (2*10GB) = 80.00	10 * (100% of 10GB + 1GB) + (2*10GB) = 130.00
Persistent disks	28.56	10 * (20% of 2GB) = 4.00	10 * (50% of 2GB) = 10.00	10 * (100% of 2GB) = 20.00

Sizing Formulas for Creating Clones When You Edit a Pool or Store Replicas on a Separate Datastore

View calculates different sizing formulas when you edit an existing desktop pool, or store replicas on a separate datastore, than when you first create a pool.

If you edit an existing pool and select datastores for the pool, View Composer creates new clones on the selected datastores. The new clones are anchored to the existing snapshot and use the existing replica disk. No new replicas are created.

View estimates the sizing requirements of new clones that are added to the desktop pool. View does not include the existing clones in the calculation.

If you store replicas on a separate datastore, the other selected datastores are dedicated to the OS disks.

Table 11-4 shows the formulas that calculate the estimated sizes of clone disks when you edit a pool or store replicas on a separate datastore.

Table 11-4. Storage Sizing Formulas for Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	Free space on the selected datastores	Number of new VMs * (2 * memory of VM)	Number of new VMs * (50% of replica disk + memory of VM)	Number of new VMs * (100% of replica disk + memory of VM)
Persistent disks	Free space on the selected datastores	Number of new VMs * 20% of persistent disk	Number of new VMs * 50% of persistent disk	Number of new VMs * 100% of persistent disk

Example of a Storage Sizing Estimate When You Edit a Pool or Store Replicas on a Separate Datastore

In this example, the parent virtual machine is configured with 1GB of memory. The parent virtual machine's disk size is 10GB. A pool is created with 10 machines. Persistent disks are configured as 2048MB in size.

The OS disks are configured on a datastore that currently has 184.23GB of available space. The persistent disks are configured on a different datastore with 28.56GB of available space.

Table 11-5 shows how the sizing formulas calculate estimated storage requirements for the sample pool.

Table 11-5. Example of a Sizing Estimate for Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	10 * (2*1GB) = 20.00	10 * (50% of 10GB + 1GB) = 60.00	10 * (100% of 10GB + 1GB) = 110.00
Persistent disks	28.56	10 * (20% of 2GB) = 4.00	10 * (50% of 2GB) = 10.00	10 * (100% of 2GB) = 20.00

Storage Overcommit for View Composer Linked-Clone Virtual Machines

With the storage overcommit feature, you can reduce storage costs by placing more linked-clone virtual machines on a datastore than is possible with full virtual machines. The linked clones can use a logical storage space several times greater than the physical capacity of the datastore.

Note Instant clones do not support storage overcommit.

This feature helps you choose a storage level that lets you overcommit the datastore's capacity and sets a limit on the number of linked clones that View creates. You can avoid either wasting storage by provisioning too conservatively or risking that the linked clones will run out of disk space and cause the operating system or applications to fail.

For example, you can create at most ten full virtual machines on a 100GB datastore, if each virtual machine is 10GB. When you create linked clones from a 10GB parent virtual machine, each clone is a fraction of that size.

If you set a conservative overcommit level, View allows the clones to use four times the physical size of the datastore, measuring each clone as if it were the size of the parent virtual machine. On a 100GB datastore, with a 10GB parent, View provisions approximately 40 linked clones. View does not provision more clones, even if the datastore has free space. This limit keeps a growth buffer for the existing clones.

Table 11-6 shows the storage overcommit levels you can set.

Table 11-6. Storage Overcommit Levels

Option	Storage Overcommit Level
None	Storage is not overcommitted.
Conservative	4 times the size of the datastore. This is the default level.
Moderate	7 times the size of the datastore.
Aggressive	15 times the size of the datastore.

Storage overcommit levels provide a high-level guide for determining storage capacity. To determine the best level, monitor the growth of linked clones in your environment.

Set an aggressive level if your OS disks will never grow to their maximum possible size. An aggressive overcommit level demands attention. To make sure that the linked clones do not run out of disk space, you can periodically refresh or rebalance the desktop pool and reduce the linked clones' OS data to its original size. Automated farms do not support refresh or rebalance. If the linked clones in an automated farm are in danger of running out of disk space, change the overcommit level.

For example, it would make sense to set an aggressive overcommit level for a floating-assignment desktop pool in which the virtual machines are set to delete or refresh after logoff.

You can vary storage overcommit levels among different types of datastores to address the different levels of throughput in each datastore. For example, a NAS datastore can have a different setting than a SAN datastore.

Set the Storage Overcommit Level for Linked-Clone Virtual Machines

You can control how aggressively View creates linked-clone virtual machines on a datastore by using the storage overcommit feature. This feature lets you create linked clones that have a total logical size larger than the physical storage limit of the datastore.

This feature works only with linked-clone pools and automated farms.

The storage overcommit level calculates the amount of storage greater than the physical size of the datastore that the clones would use if each clone were a full virtual machine. For details, see "Storage Overcommit for View Composer Linked-Clone Virtual Machines," on page 151. The following procedure applies to linked-clone desktop pools. The steps are similar for automated farms.

Procedure

1 In View Administrator, select **Catalog > Desktop Pools**.

2 When you create a new desktop pool or edit an existing pool, navigate to the vCenter Settings page.

Option	Action
New desktop pool	a Click **Add**. b Proceed through the Add Desktop Pool wizard until the vCenter Settings page appears.
Existing desktop pool	a Select the linked-clone pool and click **Edit**. b Click the **vCenter Settings** tab.

3 On the vCenter Settings page, click **Browse** next to **Datastores**.

4 Select the datastore on the Select Linked Clone Datastores page.

A drop-down menu appears in the Storage Overcommit column for the selected datastore.

5 Select the storage overcommit level from the drop-down menu.

Option	Description
None	Storage is not overcommitted.
Conservative	4 times the size of the datastore. This is the default level.
Moderate	7 times the size of the datastore.
Aggressive	15 times the size of the datastore.
Unbounded	View does not limit the number of linked-clone machines that it creates based on the physical capacity of the datastore. Select this level only if you are certain that the datastore has enough storage capacity to accommodate all of the machines and their future growth.

6 Click **OK**.

View Composer Linked-Clone Data Disks

View Composer creates more than one data disk to store the components of a linked-clone virtual machine.

OS Disk

View Composer creates an OS disk for each linked clone. This disk stores the system data that the clone needs to remain linked to the base image and to function as a unique virtual machine.

QuickPrep Configuration-Data Disk

View Composer creates a second disk with the OS disk. The second disk stores QuickPrep configuration data and other OS-related data that must be preserved during refresh and recompose operations. This disk is small, typically about 20MB. This disk is created whether you use QuickPrep or Sysprep to customize the virtual machine.

If you configure separate View Composer persistent disks to store user profiles, three disks are associated with each linked clone: the OS disk, the second virtual machine disk, and the View Composer persistent disk.

The second virtual machine disk is stored on the same datastore as the OS disk. You cannot configure this disk.

View Composer Persistent Disk

In a dedicated-assignment pool, you can configure separate View Composer persistent disks to store Windows user-profile data. This disk is optional.

Separate persistent disks let you preserve user data and settings. View Composer refresh, recompose, and rebalance operations do not affect persistent disks. You can detach a persistent disk from a linked clone and attach it to another linked clone.

If you do not configure separate persistent disks, the Windows profile is stored in the OS disk. User data and settings are removed during refresh, recompose, and rebalance operations.

You can store persistent disks on the same datastore as the OS disk or on a different datastore.

Disposable-Data Disk

When you create a linked-clone pool, you can configure a separate, nonpersistent disk to store the guest OS's paging and temp files that are generated during user sessions. You must specify the disk size in megabytes.

This disk is optional.

When the linked clone is powered off, View replaces the disposable-data disk with a copy of the original disk that View Composer created with the linked-clone pool. Linked clones can increase in size as users interact with their desktops. Using disposable-data disks can save storage space by slowing the growth of linked clones.

The disposable-data disk is stored on the same datastore as the OS disk.

Storing View Composer Linked Clones on Local Datastores

Linked-clone virtual machines can be stored on local datastores, which are internal spare disks on ESXi hosts. Local storage offers advantages such as inexpensive hardware, fast virtual-machine provisioning, high performance power operations, and simple management. However, using local storage limits the vSphere infrastructure configuration options that are available to you. Using local storage is beneficial in certain View environments but not appropriate in others.

Note The limitations described in this topic do not apply to Virtual SAN datastores, which also use local storage disks but require specific hardware.

Using local datastores is most likely to work well if the View desktops in your environment are stateless. For example, you might use local datastores if you deploy stateless kiosks or classroom and training stations.

Consider using local datastores if your virtual machines have floating assignments, are not dedicated to individual end users, do not require persistent disks for user data, and can be deleted or refreshed at regular intervals such as on user logoff. This approach lets you control the disk usage on each local datastore without having to move or load-balance the virtual machines across datastores.

However, you must consider the restrictions that using local datastores imposes on your View desktop or farm deployment:

- You cannot use VMotion to manage volumes.
- You cannot load-balance virtual machines across a resource pool. For example, you cannot use the View Composer rebalance operation with linked-clones that are stored on local datastores.
- You cannot use VMware High Availability.
- You cannot use the vSphere Distributed Resource Scheduler (DRS).
- You cannot store a View Composer replica and linked clones on separate datastores if the replica is on a local datastore.

  When you store linked clones on local datastores, VMware strongly recommends that you store the replica on the same volume as the linked clones. Although it is possible to store linked clones on local datastores and the replica on a shared datastore if all ESXi hosts in the cluster can access the replica, VMware does not recommend this configuration.
- If you select local spinning-disk drives, performance might not match that of a commercially available storage array. Local spinning-disk drives and a storage array might have similar capacity, but local spinning-disk drives do not have the same throughput as a storage array. Throughput increases as the number of spindles grows.

If you select direct attached solid-state disks (SSDs), performance is likely to exceed that of many storage arrays.

You can store linked clones on a local datastore without constraints if you configure the desktop pool or farm on a single ESXi host or a cluster that contains a single ESXi host. However, using a single ESXi host limits the size of the desktop pool or farm that you can configure.

To configure a large desktop pool or farm, you must select a cluster that contains multiple ESXi hosts with the collective capacity to support a large number of virtual machines.

If you intend to take advantage of the benefits of local storage, you must carefully consider the consequences of not having VMotion, HA, DRS, and other features available. If you manage local disk usage by controlling the number and disk growth of the virtual machines, if you use floating assignments and perform regular refresh and delete operations, you can successfully deploy linked clones to local datastores.

Storing Replicas and Clones on Separate Datastores for Instant Clones and View Composer Linked Clones

You can place replicas and clones on separate datastores with different performance characteristics. This configuration can speed up disk-intensive operations such as provisioning or running antivirus scans, especially for View Composer linked clones.

For example, you can store the replica VMs on a solid-state disk-backed datastore. Solid-state disks have low storage capacity and high read performance, typically supporting 20,000 I/Os per second (IOPS). A typical environment has only a small number of replica VMs, so replicas do not require much storage.

You can store clones on traditional, spinning media-backed datastores. These disks provide lower performance, typically supporting 200 IOPS. They are cheap and provide high storage capacity, which makes them suited for storing the a large number of clones.

Configuring replicas and clones in this way can reduce the impact of I/O storms that occur when many clones are created at once, especially for View Composer linked clones. For example, if you deploy a floating-assignment pool with a delete-machine-on-logoff policy, and your users start work at the same time, View must concurrently provision new machines for them.

Important This feature is designed for specific storage configurations provided by vendors who offer high-performance disk solutions. Do not store replicas on a separate datastore if your storage hardware does not support high-read performance.

You must follow certain requirements when you store the replica and clones in a pool on separate datastores:

- You can specify only one separate replica datastore for a pool.
- The replica datastore must be accessible from all ESXi hosts in the cluster.
- For View Composer linked clones, if the clones are on local datastores, VMware strongly recommends that you store the replica on the same volume as the linked clones. Although it is possible to store linked clones on local datastores and the replica on a shared datastore if all ESXi hosts in the cluster can access the replica, VMware does not recommend this configuration.
- This feature is not available you use Virtual SAN datastores or Virtual Volumes datastores. These types of datastores use Software Policy-Based Management, so that storage profiles define which components go on which types of disks.

Availability Considerations for Storing Replicas on a Separate Datastore

You can store replica VMs on a separate datastore or on the same datastores as the clones. These configurations affect the availability of the pool in different ways.

When you store replicas on the same datastores as the clones, to enhance availability, a separate replica is created on each datastore. If a datastore becomes unavailable, only the clones on that datastore are affected. Clones on other datastores continue to run.

When you store replicas on a separate datastore, all clones in the pool are anchored to the replicas on that datastore. If the datastore becomes unavailable, the entire pool is unavailable.

To enhance the availability of the desktop pool, you can configure a high-availability solution for the datastore on which you store the replicas.

Configure View Storage Accelerator for View Composer Linked Clones

You can configure View Composer linked-clone desktop pools to enable ESXi hosts to cache virtual machine disk data. This feature, called View Storage Accelerator, uses the Content Based Read Cache (CBRC) feature in ESXi hosts. View Storage Accelerator can reduce IOPS and improve performance during boot storms, when many machines start up or run anti-virus scans at once. The feature is also beneficial when administrators or users load applications or data frequently. To use this feature, you must make sure that View Storage Accelerator is enabled for individual desktop pools.

Note If you enable View Storage Accelerator on an existing linked-clone desktop pool, and the replica was not previously enabled for View Storage Accelerator, this feature might not take effect right away. View Storage Accelerator cannot be enabled while the replica is in use. You can force View Storage Accelerator to be enabled by recomposing the desktop pool to a new parent virtual machine. For instant clones, this feature is automatically enabled and is not configurable.

When a virtual machine is created, View indexes the contents of each virtual disk file. The indexes are stored in a virtual machine digest file. At runtime, the ESXi host reads the digest files and caches common blocks of data in memory. To keep the ESXi host cache up to date, View regenerates the digest files at specified intervals and when the virtual machine is recomposed. You can modify the regeneration interval.

You can enable View Storage Accelerator on pools that contain linked clones and pools that contain full virtual machines.

Native NFS snapshot technology (VAAI) is not supported in pools that are enabled for View Storage Accelerator.

View Storage Accelerator is enabled for a pool by default. The feature can be disabled or enabled when you create or edit a pool. The best approach is to enable this feature when you first create a desktop pool. If you enable the feature by editing an existing pool, you must ensure that a new replica and its digest disks are created before linked clones are provisioned. You can create a replica by recomposing the pool to a new snapshot or rebalancing the pool to a new datastore. Digest files can only be configured for the virtual machines in a desktop pool when they are powered off.

View Storage Accelerator is now qualified to work in configurations that use View replica tiering, in which replicas are stored on a separate datastore than linked clones. Although the performance benefits of using View Storage Accelerator with View replica tiering are not materially significant, certain capacity-related benefits might be realized by storing the replicas on a separate datastore. As a result, this combination is tested and supported.

Important If you plan to use this feature and you are using multiple View pods that share some ESXi hosts, you must enable the View Storage Accelerator feature for all pools that are on the shared ESXi hosts. Having inconsistent settings in multiple pods can cause instability of the virtual machines on the shared ESXi hosts.

Prerequisites

- Verify that your vCenter Server and ESXi hosts are version 5.0 or later.

  In an ESXi cluster, verify that all the hosts are version 5.0 or later.

- Verify that the vCenter Server user was assigned the **Host > Configuration > Advanced settings** privilege in vCenter Server. See the topics in the *View Installation* documentation that describe View and View Composer privileges required for the vCenter Server user.

- Verify that View Storage Accelerator is enabled in vCenter Server. See the *View Administration* document.

Procedure

1 In View Administrator, display the Advanced Storage Options page.

Option	Description
New desktop pool (recommended)	Start the Add Desktop Pool wizard to begin creating an automated desktop pool. Follow the wizard configuration prompts until you reach the Advanced Storage page.
Existing desktop pool	Select the existing pool, click **Edit**, and click the **Advanced Storage** tab. If you modify View Storage Accelerator settings for an existing desktop pool, the changes do not take effect until the virtual machines in the desktop pool are powered off.

2 To enable View Storage Accelerator for the pool, make sure that the **Use View Storage Accelerator** check box is selected.

This setting is selected by default. To disable the setting, uncheck the **Use View Storage Accelerator** box.

3 (Optional) Specify which disk types to cache by selecting **OS disks** only or **OS and persistent disks** from the **Disk Types** menu.

OS disks is selected by default.

If you configure View Storage Accelerator for full virtual machines, you cannot select a disk type. View Storage Accelerator is performed on the whole virtual machine.

4 (Optional) In the **Regenerate storage accelerator after** text box, specify the interval, in days, after which the regeneration for View Storage Accelerator digest files take place.

The default regeneration interval is seven days.

What to do next

You can configure blackout days and times during which disk space reclamation and View Storage Accelerator regeneration do not take place. See "Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones," on page 160.

If you enable View Storage Accelerator by editing an existing pool, recompose the desktop pool to a new snapshot or rebalance the pool to a new datastore before linked clones are provisioned.

Reclaim Disk Space on View Composer Linked Clones

In vSphere 5.1 and later, you can configure the disk space reclamation feature for View Composer linked-clone desktop pools and automated farms. Starting in vSphere 5.1, View creates linked-clone virtual machines in an efficient disk format that allows ESXi hosts to reclaim unused disk space on the linked clones, reducing the total storage space required for linked clones.

Note For instant clones, this feature is not needed because the clones are always recreated when users log off.

As users interact with the virtual machines, the linked clones' OS disks grow and can eventually use almost as much disk space as full-clone virtual machines. Disk space reclamation reduces the size of the OS disks without requiring you to refresh or recompose the linked clones. Space can be reclaimed while the virtual machines are powered on and users are interacting with the machines.

In View Administrator, you cannot directly initiate disk space reclamation for a pool. You determine when View initiates disk space reclamation by specifying the minimum amount of unused disk space that must accumulate on a linked-clone OS disk to trigger the operation. When the unused disk space exceeds the specified threshold, View directs the ESXi host to reclaim space on that OS disk. View applies the threshold to each virtual machine in the pool.

You can use the `vdmadmin -M` option to initiate disk space reclamation on a particular virtual machine for demonstration or troubleshooting purposes. See the *View Administration* document.

You can configure disk space reclamation on linked clones when you create a new pool or edit an existing pool. For an existing pool, see "Tasks for Upgrading Pools to Use Space Reclamation" in the *View Upgrades* document.

Note This feature is not available for virtual machines stored on a Virtual SAN datastore or a Virtual Volumes datastore.

If a View Composer is refreshing, recomposing, or rebalancing linked clones, disk space reclamation does not take place on those linked clones.

Disk space reclamation operates only on OS disks in linked clones. The feature does not affect View Composer persistent disks and does not operate on full-clone virtual machines.

Native NFS snapshot technology (VAAI) is not supported in pools that contain virtual machines with space-efficient disks.

The following procedure applies to linked-clone desktop pools. The steps are similar for automated farms.

Prerequisites

- Verify that your vCenter Server and ESXi hosts, including all ESXi hosts in a cluster, are version 5.1 with ESXi 5.1 download patch ESXi510-201212001 or later.
- Verify that VMware Tools that are provided with vSphere version 5.1 or later are installed on all the linked-clone virtual machines in the pool.
- Verify that all the linked-clone virtual machines in the pool are virtual hardware version 9 or later.
- Verify that the virtual machines use SCSI controllers. Disk space reclamation is not supported on virtual machines with IDE controllers.
- For Windows 10 virtual machines, verify that the machines are running in vSphere 5.5 U3 or later.
- For Windows 8 or 8.1 virtual machines, verify that the machines are running in vSphere 5.5 or later. Disk space reclamation is supported on Windows 8 or 8.1 virtual machines in vSphere 5.5 or later.
- For Windows 7 virtual machines, verify that the machines are running in vSphere 5.1 or later.
- Verify that disk space reclamation is enabled in vCenter Server. This option ensures that the virtual machines in the pool are created in the efficient disk format that is required to reclaim disk space. See the *View Administration* document.

Procedure

1 In View Administrator, display the Advanced Storage page.

Option	Description
New desktop pool	Start the Add Desktop Pool wizard to begin creating an automated desktop pool. Follow the wizard configuration prompts until you reach the Advanced Storage page.
Existing desktop pool	Select the existing pool, click **Edit**, and click the **Advanced Storage** tab. To upgrade a pool to support space reclamation, see "Upgrade Desktop Pools for Space Reclamation" in the *View Upgrades* document.

2 Select the **Reclaim VM disk space** check box.

3 In the **Initiate reclamation when unused space on VM exceeds** text box, type the minimum amount of unused disk space, in gigabytes, that must accumulate on a linked-clone OS disk before ESXi starts reclaiming space on that disk.

   For example: **2** GB.

   The default value is 1 GB.

What to do next

You can configure blackout days and times during which disk space reclamation and regeneration for View Storage Accelerator do not take place. See "Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones," on page 160.

In View Administrator, you can select **Catalog > Desktop Pools** and select a machine to display the last time space reclamation occurred and the last amount of space reclaimed on the machine.

Using VAAI Storage for View Composer Linked Clones

If your deployment includes NAS devices that support the vStorage APIs for Array Integration (VAAI), you can enable the View Composer Array Integration (VCAI) feature on View Composer linked-clone desktop pools. This feature uses native NFS snapshot technology to clone virtual machines.

NOTE In Horizon 7.0, instant clones do not support VAAI.

With this technology, the NFS disk array clones the virtual machine files without having the ESXi host read and write the data. This operation might reduce the time and network load when virtual machines are cloned.

Apply these guidelines for using native NFS snapshot technology:

- You can use this feature only if you configure desktop pools or automated farms on datastores that reside on NAS devices that support native cloning operations through VAAI.
- You can use View Composer features to manage linked clones that are created by native NFS snapshot technology. For example, you can refresh, recompose, rebalance, create persistent disks, and run QuickPrep customization scripts on these clones.
- You cannot use this feature if you store replicas and OS disks on separate datastores.
- This feature is supported on vSphere 5.0 and later.
- If you edit a pool and select or deselect the native NFS cloning feature, existing virtual machines are not affected.

  To change existing virtual machines from native NFS clones to traditional redo log clones, you must deselect the native NFS cloning feature and recompose the pool to a new base image. To change the cloning method for all virtual machines in a pool and use a different datastore, you must select the new datastore, deselect the native NFS cloning feature, rebalance the pool to the new datastore, and recompose the pool to a new base image.

  Similarly, to change virtual machines from traditional redo log clones to native NFS clones, you must select a NAS datastore that supports VAAI, select the native NFS cloning feature, rebalance the pool to the NAS datastore, and recompose the pool. For more information, see http://kb.vmware.com/kb/2088995.
- On an ESXi cluster, to configure native cloning on a selected NFS datastore in View Administrator, you might have to install vendor-specific NAS plug-ins that support native cloning operations on VAAI on all ESXi hosts in the cluster. See your storage vendor documentation for guidance on configuration requirements.

- Native NFS snapshot technology (VAAI) is not supported on virtual machines with space-efficient disks.
- This feature is not available if you use a Virtual SAN datastore or a Virtual Volumes datastore.
- See VMware Knowledge Base (KB) article 2061611 for answers to frequently asked questions about VCAI support in View.

Important NAS storage vendors might provide additional settings that can affect the performance and operation of VAAI. You should follow the vendor's recommendations and configure the appropriate settings on both the NAS storage array and ESXi. See your storage vendor documentation for guidance on configuring vendor-recommended settings.

Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones

For View Composer linked clones, regenerating digest files for View Storage Accelerator and reclaiming virtual machine disk space can use ESXi resources. To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days.

Note For instant clones, this feature is not needed.

For example, you can specify a blackout period during weekday morning hours when users start work, and boot storms and anti-virus scanning I/O storms take place. You can specify different blackout times on different days.

Disk space reclamation and View Storage Accelerator digest file regeneration do not occur during blackout times that you set. You cannot set separate blackout times for each operation.

View allows View Storage Accelerator digest files to be created for new machines during the provisioning stage, even when a blackout time is in effect.

The following procedure applies to linked-clone desktop pools. The steps are similar for automated farms.

Prerequisites

- Verify that **Enable View Storage Accelerator**, **Enable space reclamation**, or both features are selected for vCenter Server.
- Verify that **Use View Storage Accelerator**, **Reclaim VM disk space**, or both features are selected for the desktop pool.

Procedure

1. On the Advanced Storage page in the Add Desktop Pool wizard, go to **Blackout Times** and click **Add**.

   If you are editing an existing pool, click the **Advanced Storage** tab.

2. Check the blackout days and specify the starting and ending times.

   The time selector uses a 24-hour clock. For example, 10:00 is 10:00 a.m., and 22:00 is 10:00 p.m.

3. Click **OK**.
4. To add another blackout period, click **Add** and specify another period.
5. To modify or remove a blackout period, select the period from the Blackout times list and click **Edit** or **Remove**.

Configuring User Profiles with Horizon Persona Management 12

With Horizon Persona Management, you can configure user profiles that are dynamically synchronized with a remote profile repository. This feature gives users access to a personalized desktop experience whenever they log in to a desktop. Horizon Persona Management expands the functionality and improves the performance of Windows roaming profiles, but does not require Windows roaming profiles to operate.

You configure group policy settings to enable Horizon Persona Management and control various aspects of your Horizon Persona Management deployment.

To enable and use Horizon Persona Management, you must have the appropriate VMware Horizon license. See the VMware End User Licensing Agreement (EULA) at http://www.vmware.com/download/eula .

This chapter includes the following topics:

Providing User Personas in Horizon 7

With the Horizon Persona Management feature, a user's remote profile is dynamically downloaded when the user logs in to a Horizon 7 desktop. You can configure Horizon 7 to store user profiles in a secure, centralized repository. Horizon 7 downloads persona information as the user needs it.

Horizon Persona Management is an alternative to Windows roaming profiles. Horizon Persona Management expands functionality and improves performance compared to Windows roaming profiles.

You can configure and manage personas entirely within Horizon 7. You do not have to configure Windows roaming profiles. If you have a Windows roaming profiles configuration, you can use your existing repository configuration with Horizon 7.

A user profile is independent of the Horizon 7 desktop. When a user logs in to any desktop, the same profile appears.

For example, a user might log in to a floating-assignment, linked-clone desktop pool and change the desktop background and Microsoft Word settings. When the user starts the next session, the virtual machine is different, but the user sees the same settings.

A user profile comprises a variety of user-generated information:

- User-specific data and desktop settings
- Application data and settings
- Windows registry entries configured by user applications

Also, if you provision desktops with ThinApp applications, the ThinApp sandbox data can be stored in the user profile and roamed with the user.

Horizon Persona Management minimizes the time it takes to log in to and log off of desktops. Login and logoff time can be a problem with Windows roaming profiles.

- During login, Horizon 7 downloads only the files that Windows requires, such as user registry files. Other files are copied to the local desktop when the user or an application opens them from the local profile folder.
- Horizon 7 copies recent changes in the local profile to the remote repository, typically once every few minutes. The default is every 10 minutes. You can specify how often to upload the local profile.
- During logoff, only files that were updated since the last replication are copied to the remote repository.

Using Horizon Persona Management with Standalone Systems

You can install a standalone version of Horizon Persona Management on physical computers and virtual machines that are not managed by Horizon 7. With this software, you can manage user profiles across Horizon desktops and standalone systems.

The standalone Horizon Persona Management software operates on Windows 7, Windows 8, Windows 10, Windows Server 2008 R2, and Windows Server 2012 R2 operating systems.

You can use the standalone Horizon Persona Management software to accomplish these goals:

- Share user profiles across standalone systems and Horizon desktops.

  Your users can continue to use standalone systems as well as Horizon desktops with Horizon Persona Management. If you use the same Horizon Persona Management group policy settings to control Horizon desktops and physical systems, users can receive their up-to-date profiles each time they log in, whether they use their legacy computers or Horizon desktops.

  Note Horizon Persona Management does not support concurrent active sessions. A user must log out of one session before logging in to another.

- Migrate user profiles from physical systems to Horizon desktops

  If you intend to re-purpose legacy physical computers for use in a Horizon deployment, you can install standalone Horizon Persona Management on the legacy systems before you roll out Horizon desktops to your users. When users log in to their legacy systems, their profiles are stored on the Horizon remote profile repository. When users log in to their Horizon desktops for the first time, their existing profiles are downloaded to their Horizon desktops.

- Perform a staged migration from physical systems to Horizon desktops

  If you migrate your deployment in stages, users who do not yet have access to Horizon desktops can use standalone Horizon Persona Management. As each set of Horizon desktops is deployed, users can access their profiles on their Horizon desktops, and the legacy systems can be phased out. This scenario is a hybrid of the previous scenarios.

- Support up-to-date profiles when users go offline.

Users of standalone laptops can disconnect from the network. When a user reconnects, Horizon Persona Management uploads the latest changes in the user's local profile to the remote profile repository.

Note Before a user can go offline, the user profile must be completely downloaded to the local system.

Migrating User Profiles with Horizon Persona Management

With Horizon Persona Management, you can migrate existing user profiles in a variety of settings to Horizon desktops. When users log in to their Horizon desktops after a profile migration is complete, they are presented with the personal settings and data that they used on their legacy systems.

By migrating user profiles, you can accomplish the following desktop migration goals:

- You can upgrade Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops to Windows 10 Horizon desktops.
- You can upgrade your users' systems from legacy Windows XP to Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 and migrate your users from physical computers to Horizon for the first time.
- You can upgrade legacy Windows XP Horizon desktops to Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops.
- You can migrate from physical computers to Horizon desktops without upgrading the operating systems.

To support these scenarios, Horizon Persona Management provides a profile migration utility and a standalone Horizon Persona Management installer for physical or virtual machines that do not have View Agent 5.*x* installed.

Important View Agent 6.1 and later releases do not support Windows XP and Windows Vista desktops. View Agent 6.0.2 is the last release that supports these guest operating systems. Customers who have an extended support agreement with Microsoft for Windows XP and Vista, and an extended support agreement with VMware for these guest operating systems, can deploy the View Agent 6.0.2 version of their Windows XP and Vista desktops with Connection Server 6.1.

With the user profile migration utility, you can perform an important task in a migration from a legacy Windows XP desktop deployment to a desktop deployment that will continue to be supported in future releases.

Table 12-1 shows various migration scenarios and outlines the tasks you should perform in each scenario.

Table 12-1. User Profile Migration Scenarios

If This Is Your Original Deployment...	And This Is Your Destination Deployment...	Perform These Tasks:
Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops	Windows 10 Horizon desktops	1 Configure the Windows 10 Horizon desktops with Horizon Persona Management for your users. See "Configuring a Horizon Persona Management Deployment," on page 166. **Note** Do not roll out the Windows 10 Horizon desktops to your users until you complete step 2. 2 Run the View V2 to V5 profile migration utility. ■ For the source profiles, specify the remote profile repository for existing Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops. ■ For the destination profiles, specify the remote profile repository that you configured for the Windows 10 Horizon desktops. For details, see the *View User Profile Migration* document. 3 Allow your users to log in to their Windows 10 Horizon desktops.
Windows XP physical computers	Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops	1 Configure Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops with Horizon Persona Management for your users. See "Configuring a Horizon Persona Management Deployment," on page 166. **Note** Do not roll out the Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops to your users until you complete step 2. 2 Run the View V1 to V2 profile migration utility. ■ For the source profiles, specify the local profiles on the Windows XP physical computers. ■ For the destination profiles, specify the remote profile repository that you configured for the Horizon deployment. For details, see the *View User Profile Migration* document. 3 Allow your users to log in to their Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops.

Table 12-1. User Profile Migration Scenarios (Continued)

If This Is Your Original Deployment...	And This Is Your Destination Deployment...	Perform These Tasks:
Windows XP physical computers or virtual machines that use a roaming user profile solution. For example, your deployment might use one of these solutions: ■ Horizon Persona Management ■ RTO Virtual Profiles ■ Windows roaming profiles In this scenario, the original user profiles must be maintained in a remote profile repository.	Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops	1 Configure Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops with Horizon Persona Management for your users. See "Configuring a Horizon Persona Management Deployment," on page 166. **NOTE** Do not roll out the Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops to your users until you complete step 2. 2 Run the View V1 to V2 profile migration utility. ■ For the source profiles, specify the remote profile repository for the Windows XP systems. ■ For the destination profiles, specify the remote profile repository that you configured for the Horizon deployment. For details, see the *View User Profile Migration* document. 3 Allow your users to log in to their Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops.
Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 physical computers or virtual machines. The legacy systems cannot have View Agent 5.*x* installed.	Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops	1 Configure Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops with Horizon Persona Management for your users. See "Configuring a Horizon Persona Management Deployment," on page 166. 2 Install the standalone Horizon Persona Management software on the Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 systems. See "Install Standalone Horizon Persona Management," on page 170. 3 Configure the legacy Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 systems to use the same remote profile repository as the Horizon desktops. See "Configure a User Profile Repository," on page 167. The easiest approach is to use the same Horizon Persona Management group policy settings in Active Directory to control both the legacy systems and the Horizon desktops. See "Add the Horizon Persona Management ADMX or ADM Template File," on page 171. 4 Roll out your Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 Horizon desktops to your users.

Horizon Persona Management and Windows Roaming Profiles

When Horizon Persona Management is enabled, you cannot manage Horizon users' personas by using the Windows roaming profiles functions.

For example, if you log in to a desktop's guest operating system, navigate to the **Advanced** tab in the System Properties dialog box, and change the User Profiles settings from **Roaming profile** to **Local profile**, Horizon Persona Management continues to synchronize the user's persona between the local desktop and the remote persona repository.

However, you can specify files and folders within users' personas that are managed by Windows roaming profiles functionality instead of Horizon Persona Management. You use the **Windows Roaming Profiles Synchronization** policy to specify these files and folders.

Configuring a Horizon Persona Management Deployment

To configure Horizon Persona Management, you set up a remote repository that stores user profiles, install Horizon Agent with the **VMware Horizon 7 Persona Management** setup option on virtual machines that deliver remote desktop sessions, add and configure Horizon Persona Management group policy settings, and deploy desktop pools.

You can also configure Horizon Persona Management for a non-Horizon deployment. You install the standalone version of Horizon Persona Management on your users' non-Horizon laptops, desktops, or virtual machines. You must also set up a remote repository and configure Horizon Persona Management group policy settings.

Overview of Setting Up a Horizon Persona Management Deployment

To set up a Horizon desktop deployment or standalone computers with Horizon Persona Management, you must perform several high-level tasks.

This sequence is recommended, although you can perform these tasks in a different sequence. For example, you can configure or reconfigure group policy settings in Active Directory after you deploy desktop pools.

1. Configure a remote repository to store user profiles.

   You can configure a network share or use an existing Active Directory user profile path that you configured for Windows roaming profiles.

2. Install Horizon Agent with the **VMware Horizon 7 Persona Management** setup option on the virtual machines that you use to create desktop pools.

   To configure Horizon Persona Management for non-Horizon laptops, desktops, or virtual machines, install the standalone Horizon Persona Management software on each computer in your targeted deployment.

3. Add the Horizon Persona Management ADM Template file or Horizon Persona Management ADMX Template file to your Active Directory server or the Local Computer Policy configuration on the parent virtual machine.

   To configure Horizon Persona Management for your whole Horizon or non-Horizon deployment, add the ADM Template file or ADMX Template file to Active Directory.

   To configure Horizon Persona Management for one desktop pool, you can take these approaches:

   - Add the ADM Template file or ADMX Template file to the virtual machine that you use to create the pool.
   - Add the ADM Template file or ADMX Template file to Active Directory and apply the group policy settings to the OU that contains the machines in the pool.

4 Enable Horizon Persona Management by enabling the **Manage user persona** group policy setting.

5 If you configured a network share for the remote profile repository, enable the **Persona repository location** group policy setting and specify the network share path.

6 (Optional) Configure other group policy settings in Active Directory or the Local Computer Policy configuration.

7 Create desktop pools from the virtual machines on which you installed Horizon Agent with the **VMware Horizon 7 Persona Management** setup option.

Configure a User Profile Repository

You can configure a remote repository to store the user data and settings, application-specific data, and other user-generated information in user profiles. If Windows roaming profiles are configured in your deployment, you can use an existing Active Directory user profile path instead.

NOTE You can configure Horizon Persona Management without having to configure Windows roaming profiles.

Prerequisites

- Familiarize yourself with the minimum access permissions that are required to configure a shared folder. See "Setting Access Permissions on Shared Folders for Horizon Persona Management," on page 168.
- Familiarize yourself with the guidelines for creating a user profile repository. See "Creating a Network Share for Horizon Persona Management," on page 168

Procedure

1 Determine whether to use an existing Active Directory user profile path or configure a user profile repository on a network share.

Option	Action
Use an existing Active Directory user profile path	If you have an existing Windows roaming profiles configuration, you can use the user profile path in Active Directory that supports roaming profiles. You can skip the remaining steps in this procedure.
Configure a network share to store the user profile repository	If you do not have an existing Windows roaming profiles configuration, you must configure a network share for the user profile repository. Follow the remaining steps in this procedure.

2 Create a shared folder on a computer that your users can access from the guest operating systems on their desktops.

If `%username%` is not part of the folder path that you configure, Horizon Persona Management appends `%username%.%userdomain%` to the path.

For example: `\\server.domain.com\VPRepository\%username%.%userdomain%`

3 Set access permissions for the shared folders that contain user profiles.

CAUTION Make sure that access permissions are configured correctly. The incorrect configuration of access permissions on the shared folder is the most common cause of problems with Horizon Persona Management.

Setting Access Permissions on Shared Folders for Horizon Persona Management

Horizon Persona Management and Windows roaming profiles require a specific minimum level of permissions on the user profile repository. Horizon Persona Management also requires that the security group of the users who put data on the shared folder must have read attributes on the share.

Set the required access permissions on your user profile repository and redirected folder share.

Table 12-2. Minimum NTFS Permissions Required for the User Profile Repository and Redirected Folder Share

User Account	Minimum Permissions Required
Creator Owner	Full Control, Subfolders and Files Only
Administrator	None. Instead, enable the Windows group policy setting, **Add the Administrators security group to the roaming user profiles**. In the Group Policy Object Editor, this policy setting is located in **Computer Configuration\Administrative Templates\System\User Profiles**.
Security group of users needing to put data on share	List Folder/Read Data, Create Folders/Append Data, Read Attributes - This Folder Only
Everyone	No permissions
Local System	Full Control, This Folder, Subfolders and Files

Table 12-3. Share Level (SMB) Permissions Required for User Profile Repository and Redirected Folder Share

User Account	Default Permissions	Minimum Permissions Required
Everyone	Read only	No permissions
Security group of users needing to put data on share	N/A	Full Control

For information about roaming user profiles security, see the Microsoft TechNet topic, *Security Recommendations for Roaming User Profiles Shared Folders*. http://technet.microsoft.com/en-us/library/cc757013(WS.10).aspx

Creating a Network Share for Horizon Persona Management

You must follow certain guidelines when you create a shared folder to use as a profile repository.

- If you use Windows 8 desktops and your network share uses a OneFS file system on an EMC Isilon NAS device, the OneFS file system must be version 6.5.5.11 or later.
- You can create the shared folder on a server, a network-attached storage (NAS) device, or a network server.
- The shared folder does not have to be in the same domain as Horizon Connection Server.
- The shared folder must be in the same Active Directory forest as the users who store profiles in the shared folder.
- You must use a shared drive that is large enough to store the user profile information for your users. To support a large Horizon deployment, you can configure separate repositories for different desktop pools.

  If users are entitled to more than one pool, the pools that share users must be configured with the same profile repository. If you entitle a user to two pools with two different profile repositories, the user cannot access the same version of the profile from desktops in each pool.

- You must create the full profile path under which the user profile folders will be created. If part of the path does not exist, Windows creates the missing folders when the first user logs in and assigns the user's security restrictions to those folders. Windows assigns the same security restrictions to every folder it creates under that path.

  For example, for `user1` you might configure the Horizon Persona Management path `\\server\VPRepository\profiles\user1`. If you create the network share `\\server\VPRepository`, and the `profiles` folder does not exist, Windows creates the path `\profiles\user1` when `user1` logs in. Windows restricts access to the `\profiles\user1` folders to the `user1` account. If another user logs in with a profile path in `\\server\VPRepository\profiles`, the second user cannot access the repository and the user's profile fails to be replicated.

Install Horizon Agent with the Horizon Persona Management Option

To use Horizon Persona Management with Horizon desktops, you must install Horizon Agent with the **VMware Horizon 7 Persona Management** setup option on the virtual machines that you use to create desktop pools.

For an automated pool, you install Horizon Agent with the **VMware Horizon 7 Persona Management** setup option on the virtual machine that you use as a parent or template. When you create a desktop pool from the virtual machine, the Horizon Persona Management software is deployed on your Horizon desktops.

For a manual pool, you must install Horizon Agent with the **VMware Horizon 7 Persona Management** setup option on each virtual machine that is used as a desktop in the pool. Use Active Directory to configure Horizon Persona Management group policies for a manual pool. The alternative is to add the ADM template file or ADMX template file and configure group policies on each individual machine.

Prerequisites

- Verify that you are performing the installation on a Windows 7, Windows 8, Windows 10, Windows Server 2008 R2, or Windows Server 2012 R2 virtual machine. Horizon Persona Management does not operate on Microsoft RDS hosts.

  Installing Horizon Agent with the **VMware Horizon 7 Persona Management** setup option does not work on physical computers. You can install the standalone Horizon Persona Management software on physical computers. See "Install Standalone Horizon Persona Management," on page 170.

- Verify that you can log in as an administrator on the virtual machine.

- Verify that a native RTO Virtual Profiles 2.0 is not installed on the virtual machine. If a native RTO Virtual Profile 2.0 is present, uninstall it before you install Horizon Agent with the **VMware Horizon 7 Persona Management** setup option.

- Familiarize yourself with installing Horizon Agent. See "Install Horizon Agent on a Virtual Machine," on page 27 or "Install Horizon Agent on an Unmanaged Machine," on page 16.

Procedure

◆ When you install Horizon Agent on a virtual machine, select the **VMware Horizon 7 Persona Management** setup option.

What to do next

Add the Horizon Persona Management ADM template file or Horizon Persona Management ADMX template file to your Active Directory server or the Local Computer Policy configuration on the virtual machine itself. See "Add the Horizon Persona Management ADMX or ADM Template File," on page 171.

Install Standalone Horizon Persona Management

To use Horizon Persona Management with non-Horizon physical computers or virtual machines, install the standalone version of Horizon Persona Management. You can run an interactive installation or a silent installation at the command line.

Install the standalone Horizon Persona Management software on each individual computer or virtual machine in your targeted deployment.

Prerequisites

- Verify that you are performing the installation on a Windows 7, Windows 8, Windows 10, Windows Server 2008 R2, or Windows Server 2012 R2 physical computer or virtual machine. Horizon Persona Management does not operate on Windows Servers or Microsoft RDS hosts. Verify that the system satisfies the requirements described in "Supported Operating Systems for Standalone Horizon Persona Management" in the *View Installation* document.
- Verify that you can log in as an administrator on the system.
- Verify that View Agent 5.*x* or later is not installed on the computer.
- Verify that a native RTO Virtual Profiles 2.0 is not installed on the virtual machine.
- If you intend to perform a silent installation, familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 31.

Procedure

1. Download the standalone Horizon Persona Management installer file from the VMware product page at http://www.vmware.com/products/.

   The installer filename is `VMware-personamanagement-`*`y.y.y`*`-`*`xxxxxx`*`.exe` or `VMware-personamanagement-x86_64-`*`y.y.y`*`-`*`xxxxxx`*`.exe`, where *y.y.y* is the version number and *xxxxxx* is the build number.

2. Run the installation program interactively or perform a silent installation.

Option	Description
Interactive installation	a To start the installation program, double-click the installer file. b Accept the VMware license terms. c Click **Install**. By default, Horizon Persona Management is installed in the `C:\Program Files\VMware\VMware View Persona Management` directory. d Click **Finish**.
Silent installation	Open a Windows command prompt on the machine and type the installation command on one line. For example: `VMware-personamanagement-`*`y.y.y`*`-`*`xxxxxx`*`.exe /s /v"/qn /l*v ""c:\persona.log"" ALLUSERS=1"` IMPORTANT You must include the `ALLUSERS=1` property in the command line.

3. Restart your system to allow the installation changes to take effect.

What to do next

Add the Horizon Persona Management ADMX template file or ADM template file to your Active Directory or local group policy configuration.

NOTE In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

Add the Horizon Persona Management ADMX or ADM Template File

The Horizon Persona Management ADMX template file and Horizon Persona Management ADM template file contain group policy settings that allow you to configure Horizon Persona Management. Before you can configure the policies, you must add the ADMX template file or ADM template file to the local system or Active Directory server.

To configure Horizon Persona Management on a single system, you can add the group policy settings to the Local Computer Policy configuration on that local system.

To configure Horizon Persona Management for a desktop pool, you can add the group policy settings to the Local Computer Policy configuration on the virtual machine that you use as a parent or template for deploying the desktop pool.

To configure Horizon Persona Management at the domain-wide level and apply the configuration to many Horizon 7 machines or your whole deployment, you can add the group policy settings to Group Policy Objects (GPOs) on your Active Directory server. In Active Directory, you can create an OU for the Horizon 7 machines that use Horizon Persona Management, create one or more GPOs, and link the GPOs to the OU. To configure separate Horizon Persona Management policies for different types of users, you can create OUs for particular sets of Horizon 7 machines and apply different GPOs to the OUs.

For example, you might create one OU for Horizon 7 machines with Horizon Persona Management and another OU for physical computers on which the standalone Horizon Persona Management software is installed.

For an example of implementing Active Directory group policies in Horizon, see "Active Directory Group Policy Example" in the *Configuring Remote Desktop Features in Horizon 7* document.

Add the Horizon Persona Management ADM Template to a Single System

To configure Horizon Persona Management for a single desktop pool, you must add the Horizon Persona Management ADM template file to the Local Computer Policy on the virtual machine that you use to create the pool. To configure Horizon Persona Management on a single system, you must add the Horizon Persona Management ADM template file to that system.

Prerequisites

- Verify that Horizon Agent is installed with the Horizon Persona Management setup option on the system. See "Install Horizon Agent with the Horizon Persona Management Option," on page 169.
- Verify that you can log in as an administrator on the system.

Note In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

Procedure

1 Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

   The file is named `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADM and ADMX files that provide group policy settings for Horizon 7 are available in this file.

2 Unzip the file and copy the ADM file (`ViewPM.adm`) to the local system.

3 On the local system, click **Start > Run**.

4 Type **gpedit.msc** and click **OK**.

5 In the Local Computer Policy window, navigate to **Computer Configuration** and right-click **Administrative Templates**.

NOTE Do not select **Administrative Templates** under **User Configuration**.

6 Click **Add/Remove Templates** and click **Add**.

7 Browse to the directory that contains the `ViewPM.adm` file.

8 Select the `ViewPM.adm`and click **Add**.

9 Close the Add/Remove Templates window.

The Horizon Persona Management group policy settings are added to the Local Computer Policy configuration on the local system. You must use `gpedit.msc` to display this configuration.

What to do next

Configure the Horizon Persona Management group policy settings on the local system. See "Configure Horizon Persona Management Policies," on page 174.

Add the Horizon Persona Management ADM Template to Active Directory

To configure Persona Management for your deployment, you can add the Persona Management ADM template file to a Group Policy Object (GPO) in your Active Directory server.

Prerequisites

- Create GPOs for your Persona Management deployment and link them to the OU that contains the Horizon 7 machines that use Persona Management. See "Active Directory Group Policy Example" in the *Configuring Remote Desktop Features in Horizon 7* document.
- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Verify that Horizon Agent is installed with the Horizon Persona Management setup option on a system that is accessible to your Active Directory server. See "Install Horizon Agent with the Horizon Persona Management Option," on page 169.

NOTE In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

Procedure

1 Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

The file is named `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADM and ADMX files that provide group policy settings for Horizon 7 are available in this file.

2 Unzip the file and copy the Persona Management ADM file (`ViewPM.adm`), to your Active Directory server.

3 On your Active Directory server, open the Group Policy Management Console.

For example, start the Run dialog box, type **gpmc.msc**, and click **OK**.

4 In the left pane, select the domain or OU that contains your Horizon 7 machines.

5 In the right pane, right-click the GPO that you created for the group policy settings and select **Edit**.

   The Group Policy Object Editor window appears.

6 In the Group Policy Object Editor, right-click **Administrative Templates** under **Computer Configuration** and select **Add/Remove Templates**.

7 Click **Add**, browse to the `ViewPM.adm`, and click **Open**.

8 Click **Close** to apply the policy settings in the ADM template file to the GPO.

   The name of the template appears in the left pane under **Administrative Templates**.

What to do next

Configure the Persona Management group policy settings on your Active Directory server.

Add the Horizon Persona Management ADMX Template File to Active Directory or a Single System

You can add the Horizon Persona Management ADMX template file to your Active Directory server or to a single system.

Prerequisites

- Verify that Horizon Agent is installed with the Horizon Persona Management setup option. See "Install Horizon Agent with the Horizon Persona Management Option," on page 169.
- Verify that `gpedit.msc` or the appropriate group policy editor is available.

Procedure

1 Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

   The file is named `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADM and ADMX files that provide group policy settings for Horizon 7 are available in this file.

2 Unzip the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` file and copy the Horizon Persona Management ADMX files to your Active Directory server or to the individual Persona host (single system).

   a Copy the `ViewPM.admx` file to the `C:\Windows\PolicyDefinitions\` directory.

   b Copy the language resource files `ViewPM.adml` to the appropriate subfolder in `C:\Windows\PolicyDefinitions\` on your Active Directory server or the individual Persona host.

      For example, copy the `ViewPM.adml` file to the `C:\Windows\PolicyDefinitions\en-US\` directory for the EN locale.

3 On your Active Directory host, open the Group Policy Management Editor or, on an individual Persona host, open the Local Group Policy Editor with the `gpedit.msc` utility.

   The Horizon Persona Management group policy settings are installed in **Computer Configuration > Policies > Administrative Templates > Persona Management**.

What to do next

(Optional) Configure the Horizon Persona Management group policy settings. See "Configure Horizon Persona Management Policies," on page 174.

Configure Horizon Persona Management Policies

To use Horizon Persona Management, you must enable the **Manage user persona** group policy setting, which activates the Horizon Persona Management software. To set up a user profile repository without using an Active Directory user profile path, you must configure the **Persona repository location** group policy setting.

You can configure the optional group policy settings to configure other aspects of your Horizon Persona Management deployment.

If Windows roaming profiles are already configured in your deployment, you can use an existing Active Directory user profile path. You can leave the **Persona repository location** setting disabled or not configured.

Prerequisites

- Familiarize yourself with the **Manage user persona** and **Persona repository location** group policy settings. See "Roaming and Synchronization Group Policy Settings," on page 181.
- If you are setting group policies on a local system, familiarize yourself with opening the Group Policy window. See steps Step 3 and Step 4 in "Add the Horizon Persona Management ADM Template to a Single System," on page 171.
- If you are setting group policies on your Active Directory server, familiarize yourself with starting the Group Policy Object Editor. See steps Step 3 through Step 5 in "Add the Horizon Persona Management ADM Template to Active Directory," on page 172.

Procedure

1 Open the Group Policy window.

Option	Description
Local system	Open the Local Computer Policy window.
Active Directory server	Open the Group Policy Object Editor window.

2 Expand the **Computer Configuration** folder and navigate to the **Persona Management** folder.

Option	Description
Windows 7 and later or Windows Server 2008 and later	Expand the following folders: **Administrative Templates**, **Classic Administrative Templates (ADM)**, **VMware View Agent Configuration**, **Persona Management**
Windows Server 2003	Expand the following folders: **Administrative Templates**, **VMware View Agent Configuration**, **Persona Management**

3 Open the **Roaming & Synchronization** folder.

4 Double-click **Manage user persona** and click **Enabled**.

This setting activates Horizon Persona Management. When this setting is disabled or not configured, Horizon Persona Management does not function.

5 Type the profile upload interval, in minutes, and click **OK**.

The profile upload interval determines how often Horizon Persona Management copies user profile changes to the remote repository. The default upload interval is 10 minutes.

6 Double-click **Persona repository location** and click **Enabled**.

   If you have an existing Windows roaming profiles deployment, you can use an Active Directory user profile path for the remote profile repository. You do not have to configure a **Persona repository location**.

7 Type the UNC path to a network file server share that stores the user profiles.

   For example: `\\server.domain.com\UserProfilesRepository\%username%`

   The network share must be accessible to the virtual machines in your deployment.

   If you intend to use an Active Directory user profile path, you do not have to specify a UNC path.

8 If an Active Directory user profile path is configured in your deployment, determine whether to use or override this path.

Option	Action
Use the network share.	Check the **Override Active Directory user profile path if it is configured** check box.
Use an Active Directory user profile path, if one exists.	Do not check the **Override Active Directory user profile path if it is configured** check box.

9 Click **OK**.

10 (Optional) Configure other Horizon Persona Management group policy settings.

Create Desktop Pools That Use Horizon Persona Management

To use Horizon Persona Management with Horizon 7 desktops, you must create desktop pools with a Horizon Persona Management agent installed on each machine.

You cannot use Horizon Persona Management on RDS desktop pools, which run on Remote Desktop Services (RDS) hosts.

Prerequisites

- Verify that Horizon Agent with the **VMware Horizon 7 Persona Management** setup option is installed on the virtual machine that you use to create the desktop pool. See "Install Horizon Agent with the Horizon Persona Management Option," on page 169.
- If you intend to configure Horizon Persona Management policies for this desktop pool only, verify that you added the Horizon Persona Management ADM template file to the virtual machine and configured group policy settings in the Local Computer Policy configuration. See "Add the Horizon Persona Management ADM Template to a Single System," on page 171 and "Configure Horizon Persona Management Policies," on page 174.

Procedure

- Generate a snapshot or template from the virtual machine and create an automated desktop pool.

  You can configure Horizon Persona Management with pools that contain full virtual machines or linked clones. The pools can use dedicated or floating assignments.

- (Optional) To use Horizon Persona Management with manual desktop pools, select machines on which Horizon Agent with the **VMware Horizon 7 Persona Management** option is installed.

Note After you deploy Horizon Persona Management on your Horizon desktop pools, if you remove the **VMware Horizon 7 Persona Management** setup option on the Horizon machines, or uninstall Horizon Agent altogether, the local user profiles are removed from the machines of users who are not currently logged in. For users who are currently logged in, the user profiles are downloaded from the remote profile repository during the uninstall process.

Best Practices for Configuring a Horizon Persona Management Deployment

You should follow best practices for configuring Horizon Persona Management to enhance your users' desktop experience, improve desktop performance, and ensure that Horizon Persona Management operates efficiently with other Horizon 7 features.

Determining Whether to Remove Local User Profiles at Logoff

By default, Horizon Persona Management does not delete user profiles from the local machines when users log off. The **Remove local persona at log off** policy is disabled. In many cases, the default setting is a best practice because it reduces I/O operations and avoids redundant behavior.

For example, keep this policy disabled if you deploy floating-assignment pools and either refresh or delete the machines on logoff. The local profile is deleted when the virtual machine is refreshed or deleted. In a floating-assignment, automated pool, full virtual machines can be deleted after logoff. In a floating-assignment, linked-clone pool, the clones can be refreshed or deleted on logoff.

If you deploy dedicated-assignment pools, you can keep the policy disabled because users return to the same machines at each session. With the policy disabled, when a user logs in, Horizon Persona Management does not have to download files that are present in the local profile. If you configure dedicated-assignment, linked-clone pools with persistent disks, keep the policy disabled to avoid deleting user data from the persistent disks.

In some cases, you might want to enable the **Remove local persona at log off** policy.

Handling Deployments That Include Horizon Persona Management and Windows Roaming Profiles

In deployments in which Windows roaming profiles are configured, and users access Horizon desktops with Horizon Persona Management and standard desktops with Windows roaming profiles, the best practice is to use different profiles for the two desktop environments. If a Horizon desktop and the client computer from which the desktop is launched are in the same domain, and you use an Active Directory GPO to configure both Windows roaming profiles and Horizon Persona Management, enable the **Persona repository location** policy and select **Override Active Directory user profile path if it is configured**.

This approach prevents Windows roaming profiles from overwriting a Horizon Persona Management profile when the user logs off from the client computer.

If users intend to share data between existing Windows roaming profiles and Horizon Persona Management profiles, you can configure Windows folder redirection.

Configuring Paths for Redirected Folders

When you use the **Folder Redirection** group policy setting, configure the folder path to include `%username%`, but make sure that the last subfolder in the path uses the name of the redirected folder, such as `My Videos`. The last folder in the path is displayed as the folder name on the user's desktop.

For example, if you configure a path such as `\\myserver\videos\%username%\My Videos`, the folder name that appears on the user's desktop is `My Videos`.

If %username% is the last subfolder in the path, the user's name appears as the folder name. For example, instead of seeing a My Videos folder on the desktop, the user JDoe sees a folder named JDoe and cannot easily identify the folder.

Using the Windows Event Log to Monitor the Horizon Persona Management Deployment

To help you manage your deployment, Horizon Persona Management provides improved log messages and profile size and file and folder count tracking. Horizon Persona Management uses the file and folder counts to suggest folders for redirection in the Windows event log and provides statistics for these folders. For example, when a user logs in, the Windows event log might display the following suggestions to redirect folders:

```
Profile path: \\server.domain.com\persona\user1V2
...
Folders to redirect:
\\server.domain.com\persona\user1V2  Reason: Folder size larger than 1GB
\\server.domain.com\persona\user1V2\Documents  Reason: More than 10000 files and folders
```

Additional Best Practices

You can also follow these recommendations:

- By default, many antivirus products do not scan offline files. For example, when a user logs in to a desktop, these anti-virus products do not scan user profile files that are not specified in the **Files and folders to preload** or **Windows roaming profiles synchronization** group policy setting. For many deployments, the default behavior is the best practice because it reduces the I/O required to download files during on-demand scans.

  If you do want to retrieve files from the remote repository and enable scanning of offline files, see the documentation for your antivirus product.

- It is highly recommended that you use standard practices to back up network shares on which Horizon Persona Management stores the profile repository.

  Note Do not use backup software such as MozyPro or Windows Volume backup services with Horizon Persona Management to back up user profiles on Horizon desktops.

  Horizon Persona Management ensures that user profiles are backed up to the remote profile repository, eliminating the need for additional tools to back up user data on the desktops. In certain cases, tools such as MozyPro or Windows Volume backup services can interfere with Horizon Persona Management and cause data loss or corruption.

- You can set Horizon Persona Management policies to enhance performance when users start ThinApp applications. See "Configuring User Profiles to Include ThinApp Sandbox Folders," on page 178.

- If your users generate substantial persona data, and you plan to use refresh and recompose to manage dedicated-assignment, linked-clone desktops, configure your desktop pool to use separate View Composer persistent disks. Persistent disks can enhance the performance of Horizon Persona Management. See "Configuring View Composer Persistent Disks with Horizon Persona Management," on page 178.

- If you configure Horizon Persona Management for standalone laptops, make sure that the profiles are kept synchronized when users go offline. See "Manage User Profiles on Standalone Laptops," on page 179.

- Do not use Windows Client-Side Caching with Horizon Persona Management. The Windows Client-Side Caching system is a mechanism that supports the Windows Offline Files feature. If this system is in effect on the local system, Horizon Persona Management features such as folder redirection, offline file population during logon, background download, and replication of local profile files to the remote profile repository do not work properly.

  As a best practice, disable the Windows Offline Files feature before you begin using Horizon Persona Management. If you encounter issues with Horizon Persona Management because Windows Client-Side Caching is in effect on your desktops, you can resolve these issues by synchronizing the profile data that currently resides in the local Client-Side Caching database and disabling the Windows Offline Files feature. For instructions, see KB 2016416: View Persona Management features do not function when Windows Client-Side Caching is in effect.

Configuring User Profiles to Include ThinApp Sandbox Folders

Horizon Persona Management maintains user settings that are associated with ThinApp applications by including ThinApp sandbox folders in user profiles. You can set Horizon Persona Management policies to enhance performance when users start ThinApp applications.

Horizon Persona Management preloads ThinApp sandbox folders and files in the local user profile when a user logs in. The ThinApp sandbox folders are created before a user can complete the log on. To enhance performance, Horizon Persona Management does not download the ThinApp sandbox data during the login, although files are created on the local desktop with the same basic attributes and sizes as the ThinApp sandbox files in the user's remote profile.

As a best practice, download the actual ThinApp sandbox data in the background. Enable the **Folders to background download** group policy setting and add the ThinApp sandbox folders. See "Roaming and Synchronization Group Policy Settings," on page 181.

The actual ThinApp sandbox files can be large. With the **Folders to background download** setting, users do not have to wait for large files to download when they start an application. Also, users do not have to wait for the files to preload when they log in, as they might if you use the **Files and folders to preload** setting with large files.

Configuring View Composer Persistent Disks with Horizon Persona Management

With View Composer persistent disks, you can preserve user data and settings while you manage linked-clone OS disks with refresh, recompose, and rebalance operations. Configuring persistent disks can enhance the performance of Horizon Persona Management when users generate a large amount of persona information. You can configure persistent disks only with dedicated-assignment, linked-clone desktops.

Horizon Persona Management maintains each user profile on a remote repository that is configured on a network share. After a user logs into a desktop, the persona files are dynamically downloaded as the user needs them.

If you configure persistent disks with Horizon Persona Management, you can refresh and recompose the linked-clone OS disks and keep a local copy of the each user profile on the persistent disks.

The persistent disks can act as a cache for the user profiles. When a user requires persona files, Horizon Persona Management does not need to download data that is the same on the local persistent disk and the remote repository. Only unsynchronized persona data needs to be downloaded.

If you configure persistent disks, do not enable the **Remove local persona at log off** policy. Enabling this policy deletes the user data from the persistent disks when users log off.

Manage User Profiles on Standalone Laptops

If you install Horizon Persona Management on standalone (non-Horizon) laptops, make sure that the user profiles are kept synchronized when users take their standalone laptops offline.

To ensure that a standalone laptop user has an up-to-date local profile, you can configure the Horizon Persona Management group policy setting, `Enable background download for laptops`. This setting downloads the entire user profile to the standalone laptop in the background.

As a best practice, notify your users to make sure that their user profiles are completely downloaded before they disconnect from the network. Tell users to wait for the `Background download complete` notice to appear on their laptop screens before they disconnect.

To allow the `Background download complete` notice to be displayed on user laptops, configure the Horizon Persona Management group policy setting, `Show critical errors to users via tray icon alerts`.

If a user disconnects from the network before the profile download is complete, the local profile and remote profile might become unsynchronized. While the user is offline, the user might update a local file that was not fully downloaded. When the user reconnects to the network, the local profile is uploaded, overwriting the remote profile. Data that was in the original remote profile might be lost.

The following steps provide an example you might follow.

Prerequisites

Verify that Horizon Persona Management is configured for your users' standalone laptops. See "Configuring a Horizon Persona Management Deployment," on page 166.

Procedure

1 In the Active Directory OU that controls your standalone laptops, enable the `Enable background download for laptops` setting.

   In the Group Policy Object Editor, expand the following folders: **Computer Configuration**, **Administrative Templates**, **Classic Administrative Templates (ADM)**, **VMware View Agent Configuration**, **Persona Management**, **Roaming & Synchronization**.

   The **Classic Administrative Templates (ADM)** folder appears only in Windows 7 or later and Windows Server 2008 or later releases.

2 For standalone laptops, you must use a non-Horizon method to notify users when they log in.

   For example, you might distribute this message:
   `Your personal data is dynamically downloaded to your laptop after you log in. Make sure your personal data has finished downloading before you disconnect your laptop from the network. A "Background download complete" notice pops up when your personal data finishes downloading.`

Horizon Persona Management Group Policy Settings

The Horizon Persona Management ADMX template file and Horizon Persona Management ADM template file contain group policy settings that you add to the Group Policy configuration on individual systems or on an Active Directory server. You must configure the group policy settings to set up and control various aspects of Horizon Persona Management.

The ADMX template file is named `ViewPM.admx`. The ADM template file is named `ViewPM.adm`.

NOTE In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

The ADMX and ADM files are available in a bundled `.zip` file named `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`, which you can download from the VMware download site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the bundled `.zip` file.

After you add the `ViewPM.admx` or `ViewPM.adm` file to your Group Policy configuration, the policy settings are located in the **Persona Management** folder in the Group Policy window.

Table 12-4. Location of Horizon Persona Management Settings in the Group Policy Window

Operating System	Location
Windows 7 and later or Windows Server 2008 and later	**Computer Configuration** > **Administrative Templates** > **Classic Administrative Templates (ADM)** > **VMware View Agent Configuration** > **Persona Management**
Windows Server 2003	**Computer Configuration** > **Administrative Templates** > **VMware View Agent Configuration** > **Persona Management**

The group policy settings are contained in these folders:

- Roaming & Synchronization
- Folder Redirection
- Desktop UI
- Logging

Roaming and Synchronization Group Policy Settings

The roaming and synchronization group policy settings turn Horizon Persona Management on and off, set the location of the remote profile repository, determine which folders and files belong to the user profile, and control how to synchronize folders and files.

Group Policy Setting	Description
Manage user persona	Determines whether to manage user profiles dynamically with Horizon Persona Management or with Windows roaming profiles. This setting turns Horizon Persona Management on and off. When this setting is enabled, Horizon Persona Management manages user profiles. When the setting is enabled, you can specify a profile upload interval in minutes. This value determines how often changes in the user profile are copied to the remote repository. The default value is 10 minutes. When this setting is disabled or not configured, user profiles are managed by Windows.
Persona repository location	Specifies the location of the user profile repository. This setting also determines whether to use a network share that is specified in Horizon Persona Management or a path that is configured in Active Directory to support Windows roaming profiles. When this setting is enabled, you can use the **Share path** to determine the location of the user profile repository. In the **Share path** text box, you specify a UNC path to a network share that is accessible to Horizon Persona Management desktops. This setting lets Horizon Persona Management control the location of the user profile repository. For example: `\\server.domain.com\VPRepository` If `%username%` is not part of the folder path that you configure, Horizon Persona Management appends `%username%.%userdomain%` to the path. For example: `\\server.domain.com\VPRepository\%username%.%userdomain%` If you specify a location in the **Share path**, you do not have to set up roaming profiles in Windows or configure a user profile path in Active Directory to support Windows roaming profiles. For details about configuring a UNC network share for Horizon Persona Management, see "Configure a User Profile Repository," on page 167. By default, the Active Directory user profile path is used. Specifically, when the **Share path** is left blank, the Active Directory user profile path is used. The **Share path** is blank and inactive when this setting is disabled or not configured. You can also leave the path blank when this setting is enabled. When this setting is enabled, you can select the **Override Active Directory user profile path if it is configured** check box to make sure that Horizon Persona Management uses the path specified in the **Share path**. By default, this check box is unchecked, and Horizon Persona Management uses the Active Directory user profile path when both locations are configured.
Remove local persona at log off	Deletes each user's locally stored profile from the Horizon machine when the user logs off. You can also check a box to delete each user's local settings folders when the user profile is removed. Checking this box removes the `AppData\Local` folder. For guidelines for using this setting, see "Best Practices for Configuring a Horizon Persona Management Deployment," on page 176. When this setting is disabled or not configured, the locally stored user profiles, including local settings folders, are not deleted when users log off.
Roam local settings folders	Roams the local settings folders with the rest of each user profile. This policy affects the `AppData\Local` folder. By default, local settings are not roamed. You must enable this setting if you use Microsoft OneDrive.

Group Policy Setting	Description
Files and folders to preload	Specifies a list of files and folders that are downloaded to the local user profile when the user logs in. Changes in the files are copied to the remote repository as they occur. In some situations, you might want to preload specific files and folders into the locally stored user profile. Use this setting to specify these files and folders. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname. For example: `Application Data\Microsoft\Certificates` After the specified files and folders are preloaded, Horizon Persona Management manages the files and folders in the same way that it manages other profile data. When a user updates preloaded files or folders, Horizon Persona Management copies the updated data to the remote profile repository during the session, at the next profile upload interval.
Files and folders to preload (exceptions)	Prevents the specified files and folders from being preloaded. The selected folder paths must reside within the folders that you specify in the **Files and folders to preload** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Windows roaming profiles synchronization	Specifies a list of files and folders that are managed by standard Windows roaming profiles. The files and folders are retrieved from the remote repository when the user logs in. The files are not copied to the remote repository until the user logs off. For the specified files and folders, Horizon Persona Management ignores the profile replication interval that is configured by the **Profile upload interval** in the **Manage user persona** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Windows roaming profiles synchronization (exceptions)	The selected files and folders are exceptions to the paths that are specified in the **Windows roaming profiles synchronization** setting. The selected folder paths must reside within the folders that you specify in the **Windows roaming profiles synchronization** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Files and folders excluded from roaming	Specifies a list of files and folders that are not roamed with the rest of the user profile. The specified files and folders exist only on the local system. Some situations require specific files and folders to reside only in the locally stored user profile. For example, you can exclude temporary and cached files from roaming. These files do not need to be replicated to the remote repository. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname. By default, the user profile's temp folder, ThinApp cache folder, and cache folders for Internet Explorer, Firefox, Chrome, and Opera are excluded from roaming.
Files and folders excluded from roaming (exceptions)	The selected files and folders are exceptions to the paths that are specified in the **Files and folders excluded from roaming** setting. The selected folder paths must reside within the folders that you specify in the **Files and folders excluded from roaming** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Enable background download for laptops	Downloads all files in the user profile when a user logs in to a laptop on which the Horizon Persona Management software is installed. Files are downloaded in the background. When the operation is complete, a pop-up notification appears on the user's screen: `Background download complete`. To allow this notification to appear on the user's laptop, you must enable the `Show critical errors to users via tray icon alerts` setting. **NOTE** If you enable this setting, as a best practice, notify your users to make sure that the profile is completely downloaded before the users disconnect from the network. If a user takes a standalone laptop offline before the profile download is complete, the user might not have access to local profile files. While the user is offline, the user will be unable to open a local file that was not fully downloaded. See "Manage User Profiles on Standalone Laptops," on page 179.

Group Policy Setting	Description
Folders to background download	The selected folders are downloaded in the background after a user logs in to the desktop. In certain cases, you can optimize Horizon Persona Management by downloading the contents of specific folders in the background. With this setting, users do not have to wait for large files to download when they start an application. Also, users do not have to wait for the files to preload when they log in, as they might if you use the **Files and folders to preload** setting with very large files. For example, you can include VMware ThinApp sandbox folders in the **Folders to background download** setting. The background download does not affect performance when a user logs in or uses other applications on the desktop. When the user starts the ThinApp application, the required ThinApp sandbox files are likely to be downloaded from the remote repository, improving the application startup time. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Folders to background download (exceptions)	The selected folders are exceptions to the paths that are specified in the **Folders to background download** setting. The selected folder paths must reside within the folders that you specify in the **Folders to background download** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Excluded processes	The I/O of the specified processes are ignored by Horizon Persona Management. You might have to add certain anti-virus applications to the **Excluded processes** list to prevent performance problems. If an anti-virus application does not have a feature to disable offline file retrieval during its on-demand scans, the **Excluded processes** setting prevents the application from retrieving files unnecessarily. However, Horizon Persona Management does replicate changes to files and settings in the users' profiles that are made by excluded processes. To add processes to the **Excluded processes** list, enable this setting, click **Show**, type the process name, and click **OK**. For example: **`process.exe`**.
Cleanup CLFS files	Deletes the files that are generated by Common Log File System (CLFS) for `ntuser.dat` and `usrclass.dat` from the roaming profile on logon. Enable this setting only if you have to repair user profiles that are experiencing a problem with these files. Otherwise, leave the setting disabled or not configured.

Folder Redirection Group Policy Settings

With folder redirection group policy settings, you can redirect user profile folders to a network share. When a folder is redirected, all data is stored directly on the network share during the user session.

You can use these settings to redirect folders that must be highly available. Horizon Persona Management copies updates from the local user profile to the remote profile as often as once a minute, depending on the value you set for the profile upload interval. However, if a network outage or failure on the local system occurs, a user's updates since the last replication might not be saved in the remote profile. In situations where users cannot afford a temporary loss of a few minutes of recent work, you can redirect those folders that store this critical data.

The following rules and guidelines apply to folder redirection:

- When you enable this setting for a folder, you must type the UNC path of the network share to which the folder is redirected.
- If `%username%` is not part of the folder path that you configure, Horizon Persona Management appends `%username%` to the UNC path.
- As a best practice, configure the folder path to include `%username%`, but make sure that the last subfolder in the path uses the name of the redirected folder, such as `My Videos`. The last folder in the path is displayed as the folder name on the user's desktop. For details, see "Configuring Paths for Redirected Folders," on page 176.

- You configure a separate setting for each folder. You can select particular folders for redirection and leave others on the local Horizon desktop. You can also redirect different folders to different UNC paths.
- If a folder redirection setting is disabled or not configured, the folder is stored on the local Horizon desktop and managed according to the Horizon Persona Management group policy settings.
- If Horizon Persona Management and Windows roaming profiles are configured to redirect the same folder, Horizon Persona Management's folder redirection takes precedence over Windows roaming profiles.
- Folder redirection applies only to applications that use the Windows shell APIs to redirect common folder paths. For example, if an application writes a file to `%USERPROFILE%\AppData\Roaming`, the file is written to the local profile and not redirected to the network location.
- By default, Windows folder redirection gives users exclusive rights to redirected folders. To grant domain administrators access to newly redirected folders, you can use a Horizon Persona Management group policy setting.

  Windows folder redirection has a check box called **Grant user exclusive rights to *folder-name***, which gives the specified user exclusive rights to the redirected folder. As a security measure, this check box is selected by default. When this check box is selected, administrators do not have access to the redirected folder. If an administrator attempts to force change the access rights for a user's redirected folder, Horizon Persona Management no longer works for that user.

  You can make newly redirected folders accessible to domain administrators by using the **Add the administrators group to redirected folders** group policy setting. This setting lets you grant the domain administrators group full control over each redirected folder. See Table 12-5.

  For existing redirected folders, see "Granting Domain Administrators Access to Existing Redirected Folders," on page 185.

You can specify folder paths that are excluded from folder redirection. See Table 12-5.

CAUTION Horizon 7 does not support enabling folder redirection to a folder that is already in a profile managed by Horizon Persona Management. This configuration can cause failures in Horizon Persona Management and loss of user data.

For example, if the root folder in the remote profile repository is `\\Server\%username%\`, and you redirect folders to `\\Server\%username%\Desktop`, these settings would cause a failure of folder redirection in Horizon Persona Management and the loss of any contents that were previously in the `\\Server\%username%\Desktop` folder.

You can redirect the following folders to a network share:

- Application Data (roaming)
- Contacts
- Cookies
- Desktop
- Downloads
- Favorites
- History
- Links
- My Documents
- My Music

- My Pictures
- My Videos
- Network Neighborhood
- Printer Neighborhood
- Recent Items
- Save Games
- Searches
- Start Menu
- Startup Items
- Templates
- Temporary Internet Files

Table 12-5. Group Policy Settings That Control Folder Redirection

Group Policy Setting	Description
Add the administrators group to redirected folders	Determines whether to add the administrators group to each redirected folder. Users have exclusive rights to redirected folders by default. When you enable this setting, administrators can also access redirected folders. By default, this setting is not configured.
Files and Folders excluded from Folder Redirection	The selected file and folder paths are not redirected to a network share. In some scenarios, specific files and folders must remain in the local user profile. To add a folder path to the **Files and Folders excluded from Folder Redirection** list, enable this setting, click **Show**, type the path name, and click **OK**. Specify folder paths that are relative to the root of the user's local profile. For example: **`Desktop\New Folder`**.
Files and folders excluded from Folder Redirection (exceptions)	The selected file and folder paths are exceptions to the paths that are specified in the **Files and Folders excluded from Folder Redirection** setting. To add a folder path to the **Files and folders excluded from Folder Redirection (exceptions)** list, enable this setting, click **Show**, type the path name, and click **OK**. Specify folder paths that reside within a folder that is specified in the **Folders excluded from Folder Redirection** setting and are relative to the root of the user's local profile. For example: **`Desktop\New Folder\Unique Folder`**.

Granting Domain Administrators Access to Existing Redirected Folders

By default, Windows folder redirection gives users exclusive rights to redirected folders. To grant domain administrators access to existing redirected folders, you must use the `icacls` utility.

If you are setting up new redirected folders for use with View Persona Management, you can make the newly redirected folders accessible to domain administrators by using the **Add the administrators group to redirected folders** group policy setting. See Table 12-5.

Procedure

1 Set ownership for the administrator on the files and folders.

```
icacls "\\file-server\persona-share\*" /setowner "domain\admin" /T /C /L /Q
```

For example: `icacls "\\myserver-123abc\folders\*" /setowner "mycompanydomain\vcadmin" /T /C /L /Q`

2 Modify the ACLs for the files and folders.

```
icacls "\\file-server\persona-share\*" /grant "admin-group":F /T /C /L /Q
```

For example: `icacls "\\myserver-123abc\folders\*" /grant "Domain-Admins":F /T /C /L /Q`

3 For each user folder, revert ownership from the administrator to the corresponding user.

```
icacls "\\file-server\persona-share\*" /setowner "domain\folder-owner" /T /C /L /Q
```

For example: `icacls "\\myserver-123abc\folders\*" /setowner "mycompanydomain\user1" /T /C /L /Q`

Desktop UI Group Policy Settings

The desktop UI group policy settings control Horizon Persona Management settings that users see on their desktops.

Group Policy Setting	Description
Hide local offline file icon	Determines whether to hide the offline icon when a user views locally stored files that belong to the user profile. Enabling this setting hides the offline icon in Windows Explorer and most Windows dialog boxes. By default, the offline icon is hidden.
Show progress when downloading large files	Determines whether to display a progress window on a user's desktop when the client retrieves large files from the remote repository. When this setting is enabled, you can specify the minimum file size, in megabytes, to begin displaying the progress window. The window is displayed when Horizon Persona Management determines that the specified amount of data will be retrieved from the remote repository. This value is an aggregate of all files that are retrieved at one time. For example, if the setting value is 50MB and a 40MB file is retrieved, the window is not displayed. If a 30MB file is retrieved while the first file is still being downloaded, the aggregate download exceeds the value and the progress window is displayed. The window appears when a file starts downloading. By default, this value is 50MB. By default, this progress window is not displayed.
Show critical errors to users via tray icon alerts	Displays critical error icon alerts in the desktop tray when replication or network connectivity failures occur. By default, these icon alerts are hidden.

Logging Group Policy Settings

The logging group policy settings determine the name, location, and behavior of the Horizon Persona Management log files.

The following table describes each logging group policy setting.

Group Policy Setting	Description
Logging filename	Specifies the full pathname of the local Horizon Persona Management log file. The default path is `ProgramData\VMware\VDM\logs\filename`. The default logging filename is `VMWVvp.txt`.
Logging destination	Determines whether to write all log messages to the log file, the debug port, or both destinations. By default, logging messages are sent to the log file.
Logging flags	Specifies the type of log messages that are generated. ■ Log information messages. ■ Log debug messages. When this setting is disabled or not configured, and by default when the setting is configured, log messages are set to information level.

Group Policy Setting	Description
Log history depth	Determines the number of historical log files that Horizon Persona Management maintains. You can set a minimum of one and a maximum of 10 historical log files to be maintained. By default, one historical log file is maintained.
Upload log to network	Uploads the Horizon Persona Management log file to the specified network share when the user logs off. When this setting is enabled, specify the network share path. The network share path must be a UNC path. Horizon Persona Management does not create the network share. By default, the log file is not uploaded to the network share.

Troubleshooting Machines and Desktop Pools 13

You can use a variety of procedures to diagnose and fix problems that you encounter when you create and use machines and desktop pools.

Users might experience difficulty when they use Horizon Client to access desktops and applications. You can use troubleshooting procedures to investigate the causes of such problems and attempt to correct them yourself, or you can obtain assistance from VMware Technical Support.

This chapter includes the following topics:

Display Problem Machines

You can display a list of the machines whose operation View has detected as being suspect.

View Administrator displays machines that exhibit the following problems:

- Are powered on, but which are not responding.
- Remain in the provisioning state for a long time.
- Are ready, but which report that they are not accepting connections.
- Appear to be missing from a vCenter Server.
- Have active logins on the console, logins by users who are not entitled, or logins not made via a View Connection Server instance.

Procedure

1 In View Administrator, select **Resources > Machines**.

2 On the **vCenter VMs** tab, click **Problem Machines**.

What to do next

The action that you should take depends on the problem that View Administrator reports for a machine.

- If a linked-clone machine is in an error state, the View automatic recovery mechanism attempts to power on, or shut down and restart, the linked clone. If repeated recovery attempts fail, the linked clone is deleted. In certain situations, a linked clone might be repeatedly deleted and recreated. See "Troubleshooting Machines That Are Repeatedly Deleted and Recreated," on page 198.
- If a machine is powered on, but does not respond, restart its virtual machine. If the machine still does not respond, verify that the version of the Horizon Agent is supported for the machine operating system. You can use the `vdmadmin` command with the `-A` option to display the Horizon Agent version. For more information, see the *View Administration* document.
- If a machine remains in the provisioning state for a long time, delete its virtual machine, and clone it again. Verify that there is sufficient disk space to provision the machine. See "Virtual Machines Are Stuck in the Provisioning State," on page 196.
- If a machine reports that it is ready, but does not accept connections, check the firewall configuration to make sure that the display protocol is not blocked. See "Connection Problems Between Machines and Horizon Connection Server Instances," on page 203.
- If a machine appears to be missing from a vCenter Server, verify whether its virtual machine is configured on the expected vCenter Server, or if it has been moved to another vCenter Server.
- If a machine has an active login, but this is not on the console, the session must be remote. If you cannot contact the logged-in users, you might need to restart the virtual machine to forcibly log out the users.

Troubleshooting Instant Clones in the Internal VM Debug Mode

You can use the internal VM debug mode to troubleshoot internal virtual machines in instant-clone desktop pools. With the internal VM debug mode, you can analyze failed internal virtual machines before these virtual machines are deleted.

Prerequisites

- Create an instant-clone desktop pool.

Procedure

1. In the vSphere Web Client, select the master VM, and click **Manage > Configure > VM Options > Edit > VM Options > Advanced > Edit Configuration**.

   The Configuration Parameters window displays a list of parameter names and values.

2. In the Configuration Parameters window, search for the `cloneprep.debug.mode` parameter.

   If the master VM does not have the `cloneprep.debug.mode` parameter, you must add `cloneprep.debug.mode` as the parameter name and add a value of ON or OFF. If the master VM has the `cloneprep.debug.mode` parameter, you can change the value of the parameter to ON or OFF.

3. Enable or disable the internal VM debug mode for internal VMs.

   - To enable the internal VM debug mode, set the value of `cloneprep.debug.mode` to ON. If you enable the internal VM debug mode, the internal VMs are not locked and cannot be deleted by Horizon Server.
   - To disable the internal VM debug mode, set the value of `cloneprep.debug.mode` to OFF. If you disable the internal VM debug mode, the internal VMs are locked and can be deleted by Horizon Server.

   For instant clones actions such as prime, provision, resync, or unprime, the internal virtual machines use the value set in the master virtual machine. If you do not disable the internal VM debug mode, then the VMs remain in vSphere till you delete the VMs.

Restart Desktops and Reset Virtual Machines

You can perform a restart operation on a virtual desktop, which performs a graceful operating system restart of the virtual machine. You can perform a reset operation on a virtual machine without the graceful operating system restart, which performs a hard power-off and power-on of the virtual machine.

Table 13-1. Reset and Restart Functionality

Pool Type	Reset Functionality (Pools, Machines, Sessions, and Horizon Clients)	Restart Functionality (Pools, Machines, Sessions, and Horizon Clients)
Manual Pool	Reset the VM (Power Off and Power On VM)	Restart the VM (Graceful OS restart)
Full-clone pool (dedicated pool and floating pool without delete on logOff option enabled)	Reset the VM (Power Off and Power On VM)	Restart the VM (Graceful OS restart)
Full-clone pool (floating pool with delete on logOff option enabled)	**Power Off VM > Delete VM > Create new VM > Power On**	**Graceful OS shut down > Delete VM > Create new VM > Power On**
Linked-clone pool (dedicated pool and floating pool without refresh/delete on logOff option enabled)	Reset the VM (Power Off and Power On)	Restart the VM (Graceful OS restart)
Linked-clone pool (floating pool with refresh on logOff option enabled)	**Power Off VM > Refresh VM > Power On**	**Graceful OS shut down > Refresh VM > Power On**
Linked-clone pool (floating pool with refresh on logOff option enabled)	**Power Off VM > Delete VM > Create new VM > Power On**	**Graceful OS shut down > Delete VM > Create new VM > Power On**
Instant-clone pool	**Power Off VM > Delete VM > Create new VM > Power On**	**Graceful OS shut down > Delete VM > Create new VM > Power On**
Published desktop pools	NA (Not Supported)	NA (Not Supported)

Note The restart functionality is available for Horizon Clients 4.4 and later.

Procedure

1 In Horizon Administrator, select **Resources > Machines**.

2 On the **vCenter VMs** tab, choose to restart a virtual desktop or reset a virtual machine.

Option	Description
Restart Desktop	Restarts the virtual machine with a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.
Reset Virtual Machine	Resets the virtual machine without a graceful operating system restart. This action applies only to an automated pool or a manual pool that contains vCenter Server virtual machines.

3 Click **OK**.

Send Messages to Desktop Users

You might sometimes need to send messages to users who are currently logged into desktops. For example, if you need to perform maintenance on machine, you can ask the users to log out temporarily, or warn them of a future interruption of service. You can send a message to multiple users.

Procedure

1 In View Administrator, click **Catalog > Desktop Pools**.

2 Double-click a pool and click the **Sessions** tab.

3 Select one or more machines and click **Send Message**.

4 Type the message, select the message type, and click **OK**.

A message type can be **Info**, **Warning**, or **Error**.

The message is sent to all selected machines in active sessions.

Problems Provisoning or Recreating a Desktop Pool

You can use several procedures for diagnosing and fixing problems with the provisioning or recreation of desktop pools.

Instant-Clone Provisioning or Push Image Failure

The pending image of an instant-clone desktop pool is in a failed state.

Problem

During pool creation or a push image operation, the error message `Fault type is SERVER_FAULT_FATAL – Runtime error: Method called after shutdown was initiated` is displayed.

Cause

This can happen occasionally when a replica Connection Server is started while another Connection Server is doing image operations.

Solution

- If the error occurs during pool creation, enable provisioning if it is disabled. If it is enabled, disable and then enable it.
- If the error occurs during a push image operation, initiate another push image operation with the same image.

Instant Clone Image Publish Failure

View administrator shows that an image publish failed.

Problem

After creating an instant-clone desktop pool or initiating a push image, you check the status of the operation and View Administrator shows that the image publish failed.

Solution

- Re-enable provisioning if it is disabled. If it is enabled, disable and then enable it. This causes View to trigger a new Initial Publish operation.
- If it is determined that the current image has some issues, initiate another push image operation with a different image.

What to do next

If the image publish fails repeatedly, wait 30 minutes and try again.

Endless Error Recovery During Instant-Clone Provisioning

Error recovery falls into an endless loop during the provisioning of an instant-clone desktop pool

Problem

During provisioning, instant clones can go into an error state with the message "No network connection between Agent and connection Server". The automatic error recovery mechanism deletes and recreates the clones, which go into the same error state and the process repeats indefinitely.

Cause

Possible causes include a permanent network error or an incorrect path to the post-customization script.

Solution

◆ Fix any error in the network or the path to the post-customization script.

Cannot Delete Orphaned Instant Clones

On rare occasions, during provisioning, an instant clone gets into an error state and you cannot delete the desktop pool from View Administrator.

Problem

To delete the pool, View sends requests to vCenter Server to power off the clones. However, the requests fail for clones that are orphaned. The result is that View cannot delete the pool.

Solution

1 From vCenter Server, unregister the orphaned clones.

2 From View Administrator, delete the clones.

Pool Creation Fails if Customization Specifications Cannot Be Found

If you try to create a desktop pool, the operation fails if the customization specifications cannot be found.

Problem

You cannot create a desktop pool, and you see the following message in the event database.

```
Provisioning error occurred for Machine Machine_Name: Customization failed for Machine
```

Cause

The most likely cause of this problem is that you have insufficient permissions to access the customization specifications, or to create a pool. Another possible cause is that the customization specification has been renamed or deleted.

Solution

- Verify that you have sufficient permissions to access the customization specifications, and to create a pool.
- If the customization specification no longer exists because it has been renamed or deleted, choose a different specification.

Pool Creation Fails Because of a Permissions Problem

You cannot create a desktop pool if there is a permissions problem with an ESX/ESXi host, ESX/ESXi cluster, or datacenter.

Problem

You cannot create a desktop pool in View Administrator because the templates, ESX/ESXi host, ESX/ESXi cluster, or datacenter are not accessible.

Cause

This problem has a number of possible causes.

- You do not have the correct permissions to create a pool.
- You do not have the correct permissions to access the templates.
- You do not have the correct permissions to access the ESX/ESXi host, ESX/ESXi cluster, or datacenter.

Solution

- If the Template Selection screen does not show any available templates, verify that you have sufficient permissions to access the templates.
- Verify that you have sufficient permissions to access the ESX/ESXi host, ESX/ESXi cluster, or datacenter.
- Verify that you have sufficient permissions to create a pool.

Pool Provisioning Fails Due to a Configuration Problem

If a template is not available or a virtual machine image has been moved or deleted, provisioning of a desktop pool can fail.

Problem

A desktop pool is not provisioned, and you see the following message in the event database.

```
Provisioning error occurred on Pool Desktop_ID because of a configuration problem
```

Cause

This problem has a number of possible causes.

- A template is not accessible.
- The name of a template has been changed in vCenter.
- A template has been moved to a different folder in vCenter.
- A virtual machine image has been moved between ESX/ESXi hosts, or it has been deleted.

Solution

- Verify that the template is accessible.
- Verify that the correct name and folder are specified for the template.
- If a virtual machine image has been moved between ESX/ESXi hosts, move the virtual machine to the correct vCenter folder.
- If a virtual machine image has been deleted, delete the entry for the virtual machine in View Administrator and recreate or restore the image.

Pool Provisioning Fails Due to a View Connection Server Instance Being Unable to Connect to vCenter

If a Connection Server is not able to connect to vCenter, provisioning of a desktop pool can fail.

Problem

Provisioning of a desktop pool fails, and you see one of the following error messages in the event database.

- `Cannot log in to vCenter at address` *`VC_Address`*
- `The status of vCenter at address` *`VC_Address`* `is unknown`

Cause

The View Connection Server instance cannot connect to vCenter for one of the following reasons.

- The Web service on the vCenter Server has stopped.
- There are networking problems between the View Connection Server host and the vCenter Server.
- The port numbers and login details for vCenter or View Composer have changed.

Solution

- Verify that the Web service is running on the vCenter.
- Verify that there are no network problems between the View Connection Server host and the vCenter.
- In View Administrator, verify the port numbers and login details that are configured for vCenter and View Composer.

Pool Provisioning Fails Due to Datastore Problems

If a datastore is out of disk space, or you do not have permission to access the datastore, provisioning of a desktop pool can fail.

Problem

Provisioning of a desktop pool fails, and you see one of the following error messages in the event database.

- `Provisioning error occurred for Machine` *`Machine_Name`*`: Cloning failed for Machine`
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because available free disk space is reserved for linked clones`
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because of a resource problem`

Cause

You do not have permission to access the selected datastore, or the datastore being used for the pool is out of disk space.

Solution

- Verify that you have sufficient permissions to access the selected datastore.
- Verify whether the disk on which the datastore is configured is full.
- If the disk is full or the space is reserved, free up space on the disk, rebalance the available datastores, or migrate the datastore to a larger disk.

Pool Provisioning Fails Due to vCenter Server Being Overloaded

If vCenter Server is overloaded with requests, provisioning of a desktop pool can fail.

Problem

Provisioning of a desktop pool fails, and you see the following error message in the event database.

```
Provisioning error occurred on Pool Desktop_ID because of a timeout while customizing
```

Cause

vCenter is overloaded with requests.

Solution

- In View Administrator, reduce the maximum number of concurrent provisioning and power operations for vCenter Server.
- Configure additional vCenter Server instances.

  For more information about configuring vCenter Server, see the *View Installation* document.

Virtual Machines Are Stuck in the Provisioning State

After being cloned, virtual machines are stuck in the Provisioning state.

Problem

Virtual machines are stuck in the Provisioning state.

Cause

The most likely cause of this problem is that you restarted the View Connection Server instance during a cloning operation.

Solution

◆ Delete the virtual machines and clone them again.

Virtual Machines Are Stuck in the Customizing State

After being cloned, virtual machines are stuck in the Customizing state.

Problem

Virtual machines are stuck in the Customizing state.

Cause

The most likely cause of this problem is that there is not enough disk space to start the virtual machine. A virtual machine must start before customization can take place.

Solution

- Delete the virtual machine to recover from a stuck customization.
- If the disk is full, free up space on the disk or migrate the datastore to a larger disk.

Removing Orphaned or Deleted Linked Clones

Under certain conditions, linked-clone data in View, View Composer, and vCenter Server might get out of synchronization, and you might be unable to provision or delete linked-clone machines.

Problem

- You cannot provision a linked-clone desktop pool.
- Provisioning linked-clone machines fails, and the following error occurs: `Virtual machine with Input Specification already exists`
- In View Administrator, linked-clone machines are stuck in a `Deleting` state. You cannot restart the Delete command in View Administrator because the machines are already in the `Deleting` state.

Cause

This issue occurs if the View Composer database contains information about linked clones that is inconsistent with the information in View LDAP, Active Directory, or vCenter Server. Several situations can cause this inconsistency:

- The linked-clone virtual machine name is changed manually in vCenter Server after the pool was created, causing View Composer and vCenter Server refer to the same virtual machine with different names.
- A storage failure or manual operation causes the virtual machine to be deleted from vCenter Server. The linked-clone virtual machine data still exists in the View Composer database, View LDAP, and Active Directory.
- While a pool is being deleted from View Administrator, a networking or other failure leaves the virtual machine in vCenter Server.

Solution

If the virtual machine name was renamed in vSphere Client after the desktop pool was provisioned, try renaming the virtual machine to the name that was used when it was deployed in View.

If other database information is inconsistent, use the `SviConfig RemoveSviClone` command to remove these items:

- The linked clone database entries from the View Composer database
- The linked clone machine account from Active Directory
- The linked clone virtual machine from vCenter Server

The `SviConfig` utility is located with the View Composer application. The default path is `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`.

IMPORTANT Only experienced View Composer administrators should use the `SviConfig` utility. This utility is intended to resolve issues relating to the View Composer service.

Take these steps:

1 Verify that the View Composer service is running.

2 From a Windows command prompt on the View Composer computer, run the `SviConfig RemoveSviClone` command in the following form:

```
sviconfig -operation=removesviclone
          -VmName=virtual machine name
          [-AdminUser=local administrator username]
          -AdminPassword=local administrator password
          [-ServerUrl=View Composer server URL]
```

For example:

```
sviconfig -operation=removesviclone -vmname=MyLinkedClone
 -adminuser=Admin -adminpassword=Pass -serverurl=ViewComposerURL
```

The `VmName` and `AdminPassword` parameters are required. The default value of the `AdminUser` parameter is `Administrator`. The default value of the `ServerURL` parameter is `https://localhost:18443/SviService/v2_0`

For more information about removing virtual machine information from View LDAP, see VMware Knowledge Base article 2015112: *Manually deleting linked clones or stale virtual desktop entries from the View Composer database in VMware View Manager and VMware Horizon View*.

Troubleshooting Machines That Are Repeatedly Deleted and Recreated

View can repeatedly delete and recreate linked-clone and full-clone machines that are in an Error state.

Problem

A linked-clone or full-clone machine is created in an Error state, deleted, and recreated in an Error state. This cycle keeps repeating.

Cause

When a large desktop pool is provisioned, one or more virtual machines might end up in an Error state. The View automatic recovery mechanism attempts to power on the failed virtual machine. If the virtual machine does not power on after a certain number of attempts, View deletes the virtual machine.

Following the pool size requirements, View creates a new virtual machine, often with the same machine name as the original machine. If the new virtual machine is provisioned with the same error, that virtual machine is deleted, and the cycle repeats.

Automatic recovery is performed on linked-clone and full-clone machines.

If automatic recovery attempts fail for a virtual machine, View deletes the virtual machine only if it is a floating machine or a dedicated machine that is not assigned to a user. Also, View does not delete virtual machines when pool provisioning is disabled.

Solution

Examine the parent virtual machine or template that was used to create the desktop pool. Check for errors in the virtual machine or guest operating system that might cause the error in the virtual machine.

For linked clones, resolve errors in the parent virtual machine and take a new snapshot.

- If many machines are in an Error state, use the new snapshot or template to recreate the pool.
- If most machines are healthy, select the desktop pool in View Administrator, click **Edit**, select the vCenter Settings tab, select the new snapshot as a default base image, and save your edits.

  New linked-clone machines are created using the new snapshot.

For full clones, resolve errors in the virtual machine, generate a new template, and recreate the pool.

Troubleshooting QuickPrep Customization Problems

A View Composer QuickPrep customization script can fail for a variety of reasons.

Problem

A QuickPrep post-synchronization or power-off script does not execute. In some cases, a script might complete successfully on some linked clones, but fail on others.

Cause

A few common causes exist for QuickPrep script failures:

- The script times out
- The script path refers to a script that requires an interpreter
- The account under which the script runs does not have sufficient permission to execute a script task

Solution

- Examine the customization script log.

  QuickPrep customization information is written to a log file in Windows `temp` directory:

  ```
  C:\Windows\Temp\vmware-viewcomposer-ga-new.log
  ```

- Determine if the script timed out.

  View Composer terminates a customization script that takes longer than 20 seconds. The log file displays a message showing that the script has started and a later message indicating the timeout:

  ```
  2010-02-21 21:05:47,687 [1500] INFO Ready -
  [Ready.cpp, 102] Running the PostSync script: cmd /c
  C:\temp\build\composer.bat
  2010-02-21 21:06:07,348 [1500] FATAL Guest -
  [Guest.cpp, 428] script cmd /c
  C:\temp\build\composer.bat timed out
  ```

  To solve a timeout problem, increase the timeout limit for the script and run it again.

- Determine if the script path is valid.

  If you use a scripting language that needs an interpreter to execute the script, the script path must start with the interpreter binary.

  For example, if you specify the path `C:\script\myvb.vbs` as a QuickPrep customization script, View Composer Agent cannot execute the script. You must specify a path that starts with the interpreter binary path:

  ```
  C:\windows\system32\cscript.exe c:\script\myvb.vbs
  ```

- Determine if the account under which the script runs has appropriate permissions to perform script tasks.

  QuickPrep runs the scripts under the account under which the VMware View Composer Guest Agent Server service is configured to run. By default, this account is `Local System`.

  Do not change this log on account. If you do, the linked clones do not start.

Finding and Unprotecting Unused View Composer Replicas

Under certain conditions, View Composer replicas might remain in vCenter Server when they no longer have any linked clones associated with them.

Problem

An unused replica remains in a vCenter Server folder. You are unable to remove the replica by using vSphere Client.

Cause

Network outages during View Composer operations, or removing the associated linked clones directly from vSphere without using the proper View commands, might leave an unused replica in vCenter Server.

Replicas are protected entities in vCenter Server. They cannot be removed by ordinary vCenter Server or vSphere Client management commands.

Solution

Use the `SviConfig FindUnusedReplica` command to find the replica in a specified folder. You can use the `-Move` parameter to move the replica to another folder. The `-Move` parameter unprotects an unused replica before moving it.

IMPORTANT Only experienced View Composer administrators should use the `SviConfig` utility. This utility is intended to resolve issues relating to the View Composer service.

The `SviConfig` utility is located with the View Composer application. The default path is `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`.

Before you begin, verify that no linked clones are associated with the replica.

Familiarize yourself with the `SviConfig FindUnusedReplica` parameters:

- `DsnName`. The DSN that must be used to connect to the database.
- `UserName`. The user name used to connect to the database. If this parameter is not specified, Windows authentication is used.
- `Password`. The password for the user that connects to the database. If this parameter is not specified and Windows authentication is not used, you are prompted to enter the password later.
- `ReplicaFolder`. The name of the replica folder. Use an empty string for the root folder. The default value is `VMwareViewComposerReplicaFolder`.
- `UnusedReplicaFolder`. The name of the folder to contain all unused replicas. The default value is `UnusedViewComposerReplicaFolder`. Use this parameter to specify the destination folder when you use the `Move` parameter.
- `OutputDir`. The name of the output directory in which the list of unused replicas, stored in the `unused-replica-*.txt` file, is generated. The default value is the current working directory.
- `Move`. Determines whether to unprotect unused replica virtual machines and move them to a specified folder. The `UnusedReplicaFolder` parameter specifies the destination folder. The default value of the `Move` parameter is `false`.

The `DsnName`, `Username`, and `Password` parameters are required. The `DsnName` cannot be an empty string.

Take these steps:

1 Stop the View Composer service.

2 From a Windows command prompt on the View Composer computer, run the `SviConfig FindUnusedReplica` command in the following form:

```
sviconfig -operation=findunusedreplica
          -DsnName=name of the DSN
          -Username=Database administrator username
          -Password=Database administrator password
          [-ReplicaFolder=Replica folder name]
          [-UnusedReplicaFolder=Unused replica folder name.]
          [-OutputDir=Output file directory]
          [-Move=true or false]
```

For example:

```
sviconfig -operation=FindUnusedReplica -DsnName=SVI
   -Username=SVIUser -Password=1234 -Move=True
```

3 Restart the View Composer service.

4 (Optional) After the replica is moved to the new folder, remove the replica virtual machine from vCenter Server.

View Composer Provisioning Errors

If an error occurs when View Composer provisions or recomposes linked-clone machines, an error code indicates the cause of the failure. The error code appears in the machine-status column in View Administrator.

Table 13-2 describes the View Composer provisioning error codes.

This table lists errors that are associated with View Composer and QuickPrep customization. Additional errors can occur in View Connection Server and other View components that can interfere with machine provisioning.

Table 13-2. View Composer Provisioning Errors

Error	Description
0	The policy was applied successfully. **Note** Result code 0 does not appear in View Administrator. The linked-clone machine proceeds to a Ready state, unless a View error outside the domain of View Composer occurs. This result code is included for completeness.
1	Failed to set the computer name.
2	Failed to redirect the user profiles to the View Composer persistent disk.
3	Failed to set the computer's domain account password.
4	Failed to back up a user's profile keys. The next time the user logs in to this linked-clone machine after the recompose operation, the OS creates a new profile directory for the user. As a new profile is created, the user cannot not see the old profile data.
5	Failed to restore a user's profile. The user should not log in to the machine in this state because the profile state is undefined.

Table 13-2. View Composer Provisioning Errors (Continued)

Error	Description
6	Errors not covered by other error codes. The View Composer agent log files in the guest OS can provide more information about the causes of these errors. For example, a Windows Plug and Play (PnP) timeout can generate this error code. In this situation, View Composer times out after waiting for the PnP service to install new volumes for the linked-clone virtual machine. PnP mounts up to three disks, depending on how the pool was configured: ■ View Composer persistent disk ■ Nonpersistent disk for redirecting guest OS temp and paging files ■ Internal disk that stores QuickPrep configuration and other OS-related data. This disk is always configured with a linked clone. The timeout length is 10 minutes. If PnP does not finish mounting the disks within 10 minutes, View Composer fails with error code 6.
7	Too many View Composer persistent disks are attached to the linked clone. A clone can have at most three View Composer persistent disks.
8	A persistent disk could not be mounted on the datastore that was selected when the pool was created.
9	View Composer could not redirect disposable-data files to the nonpersistent disk. Either the paging file or the temp-files folders were not redirected.
10	View Composer cannot find the QuickPrep configuration policy file on the specified internal disk.
12	View Composer cannot find the internal disk that contains the QuickPrep configuration policy file and other OS-related data.
13	More than one persistent disk is configured to redirect the Windows user profile.
14	View Composer failed to unmount the internal disk.
15	The computer name that View Composer read from configuration-policy file does not match the current system name after the linked clone is initially powered on.
16	The View Composer agent did not start because the volume license for the guest OS was not activated.
17	The View Composer agent did not start. The agent timed out while waiting for Sysprep to start.
18	The View Composer agent failed to join the linked-clone virtual machine to a domain during customization.
19	The View Composer agent failed to execute a post-synchronization script.
20	The View Composer agent failed to handle a machine password synchronization event. This error might be transient. If the linked clone joins the domain, the password is fine. If the clone fails to join the domain, restart the operation you performed before the error occurred. If you restarted the clone, restart it again. If you refreshed the clone, refresh it again. If the clone still fails to join the domain, recompose the clone.
21	The View Composer agent failed to mount the system disposable disk.
22	The View Composer agent failed to mount the View Composer persistent disk.

Troubleshooting Network Connection Problems

You can use a variety of procedures for diagnosing and fixing problems with network connections with machines, Horizon Client devices, and View Connection Server instances.

Connection Problems Between Machines and Horizon Connection Server Instances

You might experience connection problems between machines and Horizon Connection Server instances.

Problem

If connectivity between a machine and a Connection Server instance fails, you see one of the following messages in the event database.

- `Provisioning error occurred for Machine` *`Machine_Name`*`: Customization error due to no network communication between the Horizon Agent and Connection Server`
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because of a networking problem with a Horizon Agent`
- `Unable to launch from Pool` *`Desktop_ID`* `for user` *`User_Display_Name`*`: Failed to connect to Machine` *`MachineName`* `using` *`Protocol`*

Cause

The connectivity problems between a machine and a Connection Server instance can occur for different reasons.

- Lookup failure on the machine for the DNS name of the Connection Server host.
- The ports for JMS, RDP, or AJP13 communication being blocked by firewall rules.
- The failure of the JMS router on the Connection Server host.

Solution

- At a command prompt on the machine, type the `nslookup` command.

  ```
  nslookup CS_FQDN
  ```

  CS_FQDN is the fully qualified domain name (FQDN) of the Connection Server host. If the command fails to return the IP address of the Connection Server host, apply general network troubleshooting techniques to correct the DNS configuration.

- At a command prompt on the machine, verify that TCP port 4001, which Horizon Agent uses to establish JMS communication with the Connection Server host, is working by typing the `telnet` command.

  ```
  telnet CS_FQDN 4001
  ```

  If the `telnet` connection is established, network connectivity for JMS is working.

- If a security server is deployed in the DMZ, verify that exception rules are configured in the inner firewall to allow RDP connectivity between the security server and virtual machines on TCP port 3389.
- If secure connections are bypassed, verify that the firewall rules allow a client to establish either a direct RDP connection to the virtual machine on TCP port 3389, or a direct PCoIP connection to the virtual machine on TCP port 4172 and UDP port 4172.
- Verify that exception rules are configured in the inner firewall to allow connections between each Security Server and its associated Connection Server host on TCP port 4001 (JMS) and TCP port 8009 (AJP13).

Connection Problems Between Horizon Client and the PCoIP Secure Gateway

You might experience connection problems between Horizon Client and a security server or Horizon Connection Server host when the PCoIP Secure Gateway is configured to authenticate external users that communicate over PCoIP.

Problem

Clients that use PCoIP cannot connect to or display Horizon 7 desktops. The initial login to a security server or Connection Server instance succeeds, but the connection fails when the user selects a Horizon 7 desktop. This issue occurs when the PCoIP Secure Gateway is configured on a security server or Connection Server host.

Note Typically, the PCoIP Secure Gateway is leveraged on a security server. In a network configuration in which external clients connect directly to a Horizon Connection Server host, the PCoIP Secure Gateway can also be configured on Connection Server.

Cause

Problems connecting to the PCoIP Secure Gateway can occur for different reasons.

- Windows Firewall has closed a port that is required for the PCoIP Secure Gateway.
- The PCoIP Secure Gateway is not enabled on the security server or Horizon Connection Server instance.
- The PCoIP External URL setting is configured incorrectly. You must specify this setting as the external IP address that clients can access over the Internet.
- The PCoIP External URL, secure tunnel External URL, Blast External URL, or another address is configured to point to a different security server or Connection Server host. When you configure these addresses on a security server or Connection Server host, all addresses must allow client systems to reach the current host.
- The client is connecting through an external web proxy that has closed a port required for the PCoIP Secure Gateway. For example, a web proxy in a hotel network or public wireless connection might block the required ports.
- The Connection Server instance that is paired with the security server on which the PCoIP Secure Gateway is configured is version View 4.5 or earlier. The security server and paired Connection Server instance must be View 4.6 or later.

Solution

- Check that the following network ports are opened on the firewall for the security server or Connection Server host.

Port	Description
TCP 4172	From Horizon Client to the security server or Connection Server host.
UDP 4172	Between Horizon Client and the security server or Connection Server host, in both directions.
TCP 4172	From the security server or Connection Server host to the Horizon 7 desktop.
UDP 4172	Between the security server or Connection Server host and the Horizon 7 desktop, in both directions.

- In Horizon Administrator, make sure that the PCoIP Secure Gateway is enabled.

  a Click **View Configuration > Servers**.

  b Select the Connection Server instance on the **Connection Servers** tab and click **Edit**.

c Select **Use PCoIP Secure Gateway for PCoIP connections to machine**.

  The PCoIP Secure Gateway is disabled by default.

d Click **OK**.

- In Horizon Administrator, make sure that the PCoIP External URL is configured correctly.

  a Click **View Configuration > Servers**.

  b Select the host to configure.

  - If your users connect to the PCoIP Secure Gateway on a security server, select the security server on the **Security Servers** tab.
  - If your users connect to the PCoIP Secure Gateway on a Connection Server instance, select that instance on the **Connection Servers** tab.

  c Click **Edit**.

  d In the **PCoIP External URL** text box, make sure that the URL contains the external IP address for the security server or Connection Server host that clients can access over the Internet.

  Specify port 4172. Do not include a protocol name.

  For example: `10.20.30.40:4172`

  e Make sure that all addresses in this dialog allow client systems to reach this host.

  All addresses in the Edit Security Server Settings dialog must allow client systems to reach this security server host. All addresses in the Edit Connection Server Settings dialog must allow client systems to reach this Connection Server instance.

  f Click **OK**.

  Repeat these steps for each security server and Connection Server instance on which users connect to the PCoIP Secure Gateway.

- If the user is connecting through a web proxy that is outside of your network, and the proxy is blocking a required port, direct the user to connect from a different network location.

Connection Problems Between Machines and Horizon Connection Server Instances

You might experience connection problems between machines and Horizon Connection Server instances.

Problem

If connectivity between a machine and a Connection Server instance fails, you see one of the following messages in the event database.

- `Provisioning error occurred for Machine` *`Machine_Name`*`: Customization error due to no network communication between the Horizon Agent and Connection Server`
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because of a networking problem with a Horizon Agent`
- `Unable to launch from Pool` *`Desktop_ID`* `for user` *`User_Display_Name`*`: Failed to connect to Machine` *`MachineName`* `using` *`Protocol`*

Cause

The connectivity problems between a machine and a Connection Server instance can occur for different reasons.

- Lookup failure on the machine for the DNS name of the Connection Server host.

- The ports for JMS, RDP, or AJP13 communication being blocked by firewall rules.
- The failure of the JMS router on the Connection Server host.

Solution

- At a command prompt on the machine, type the `nslookup` command.

  ```
  nslookup CS_FQDN
  ```

  CS_FQDN is the fully qualified domain name (FQDN) of the Connection Server host. If the command fails to return the IP address of the Connection Server host, apply general network troubleshooting techniques to correct the DNS configuration.
- At a command prompt on the machine, verify that TCP port 4001, which Horizon Agent uses to establish JMS communication with the Connection Server host, is working by typing the `telnet` command.

  ```
  telnet CS_FQDN 4001
  ```

  If the `telnet` connection is established, network connectivity for JMS is working.
- If a security server is deployed in the DMZ, verify that exception rules are configured in the inner firewall to allow RDP connectivity between the security server and virtual machines on TCP port 3389.
- If secure connections are bypassed, verify that the firewall rules allow a client to establish either a direct RDP connection to the virtual machine on TCP port 3389, or a direct PCoIP connection to the virtual machine on TCP port 4172 and UDP port 4172.
- Verify that exception rules are configured in the inner firewall to allow connections between each Security Server and its associated Connection Server host on TCP port 4001 (JMS) and TCP port 8009 (AJP13).

Connection Problems Due to Incorrect Assignment of IP Addresses to Cloned Machines

You might not be able to connect to cloned machines if they have static IP addresses.

Problem

You cannot use Horizon Client to connect to cloned machines.

Cause

Cloned machines are incorrectly configured to use a static IP address instead of using DHCP to obtain their IP addresses.

Solution

1. Verify that the template for a desktop pool on vCenter Server is configured to use DHCP to assign IP addresses to machines.
2. In the vSphere Web Client, clone one virtual machine manually from the desktop pool and verify that it obtains its IP address from DHCP correctly.

Troubleshooting USB Redirection Problems

Various problems can arise with USB redirection in Horizon Client.

Problem

USB redirection in Horizon Client fails to make local devices available on the remote desktop, or some devices do not appear to be available for redirection in Horizon Client.

Cause

The following are possible causes for USB redirection failing to function correctly or as expected.

- The device is a composite USB device and one of the devices it includes is blocked by default. For example, a dictation device that includes a mouse is blocked by default because mouse devices are blocked by default. To work around this problem, see "Configuring Device Splitting Policy Settings for Composite USB Devices" in the *Configuring Remote Desktop Features in Horizon 7* document.
- USB redirection is not supported on Windows Server 2008 RDS hosts that deploy remote desktops and applications. USB redirection is supported on Windows Server 2012 RDS hosts with View Agent 6.1 and later, but only for USB storage devices. USB redirection is supported on Windows Server 2008 R2 and Windows Server 2012 R2 systems that are used as single-user desktops.
- Only USB flash drives and hard disks are supported on RDS desktops and applications. You cannot redirect other types of USB devices, and other types of USB storage devices such as security storage drives and USB CD-ROM, to an RDS desktop or application.
- Webcams are not supported for redirection.
- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle.
- USB redirection is not supported for boot devices. If you run Horizon Client on a Windows system that boots from a USB device, and you redirect this device to the remote desktop, the local operating system might become unresponsive or unusable. See http://kb.vmware.com/kb/1021409.
- By default, Horizon Client for Windows does not allow you to select keyboard, mouse, smart card and audio-out devices for redirection. See http://kb.vmware.com/kb/1011600.
- RDP does not support the redirection of USB HIDs for the console session, or of smart card readers. See http://kb.vmware.com/kb/1011600.
- Windows Mobile Device Center can prevent the redirection of USB devices for RDP sessions. See http://kb.vmware.com/kb/1019205.
- For some USB HIDs, you must configure the virtual machine to update the position of the mouse pointer. See http://kb.vmware.com/kb/1022076.
- Some audio devices might require changes to policy settings or to registry settings. See http://kb.vmware.com/kb/1023868.
- Network latency can cause slow device interaction or cause applications to appear frozen because they are designed to interact with local devices. Very large USB disk drives might take several minutes to appear in Windows Explorer.
- USB flash cards formatted with the FAT32 file system are slow to load. See http://kb.vmware.com/kb/1022836.
- A process or service on the local system opened the device before you connected to the remote desktop or application.
- A redirected USB device stops working if you reconnect a desktop or application session even if the desktop or application shows that the device is available.
- USB redirection is disabled in View Administrator.
- Missing or disabled USB redirection drivers on the guest.

Solution

- If available, use PCoIP instead of RDP as the protocol.
- If a redirected device remains unavailable or stops working after a temporary disconnection, remove the device, plug it in again, and retry the redirection.

- In View Administrator, go to **Policies > Global Policies**, and verify that USB access is set to **Allow** under View Policies.
- Examine the log on the guest for entries of class `ws_vhub`, and the log on the client for entries of class `vmware-view-usbd`.

  Entries with these classes are written to the logs if a user is not an administrator, or if the USB redirection drivers are not installed or are not working. For the location of these log files, see "Using Log Files for Troubleshooting and to Determine USB Device IDs" in the *Configuring Remote Desktop Features in Horizon 7* document.
- Open the Device Manager on the guest, expand Universal Serial Bus controllers, and reinstall the VMware View Virtual USB Host Controller and VMware View Virtual USB Hub drivers if these drivers are missing or re-enable them if they are disabled.

Manage Machines and Policies for Unentitled Users

You can display the machines that are allocated to users whose entitlement has been removed, and you can also display the policies that have been applied to unentitled users.

A user who is unentitled might have left the organization permanently, or you might have suspended their account for an extended period of time. These users are assigned a machine but they are no longer entitled to use the machine pool.

You can also use the `vdmadmin` command with the `-O` or `-P` option to display unentitled machines and policies. For more information, see the *View Administration* document.

Procedure

1. In View Administrator, select **Resources > Machines**.
2. Select **More Commands > View Unentitled Machines**.
3. Remove the machine assignments for unentitled users.
4. Select **More Commands > View Unentitled Machines** or **More Commands > View Unentitled Policies** as appropriate.
5. Change or remove the policies that are applied to unentitled users.

Resolving Database Inconsistencies with the ViewDbChk Command

With the `ViewDbChk` command, you can resolve inconsistencies in the databases that store information about desktop virtual machines in an automated desktop pool and RDS hosts in an automated farm.

In a View environment, information about desktop virtual machines and RDS hosts in an automated farm is stored in the following places:

- The LDAP database
- The vCenter Server database
- For View Composer linked-clone machines only: the View Composer database

Normally, you can recover from an error that occurs during provisioning or other operations by removing or resetting a desktop virtual machine or an RDS host using View Administrator. On rare occasions, the information in the different databases about a machine that is in an error state might become inconsistent and it is not possible to recover from the error using View Administrator. You might see one of the following symptoms:

- Provisioning fails with the error message `Virtual machine with Input Specification already exists`.
- Recomposing a desktop pool fails with the error message `Desktop Composer Fault: Virtual Machine with Input Specification already exists`.

- View Administrator shows that a desktop machine or an RDS host is stuck in a deleting state.
- You cannot delete a desktop pool or an automated farm.
- You cannot delete a desktop machine or an RDS host.
- In View Administrator's Inventory tab, the status of a desktop machine or an RDS host is missing.

In situations where database inconsistencies cause a desktop machine or an RDS host to be in an unrecoverable error state or prevent a View Administrator task from completing successfully, you can use the `ViewDbChk` command to resolve the inconsistencies. The `ViewDbChk` command has the following characteristics:

- `ViewDbChk` is automatically installed when you install View Standard Server or View Replica Server. The utility is not installed when you install View Security Server.
- `ViewDbChk` is a command that you can run from the Windows Command Prompt or from a script.
- `ViewDbChk` supports automated farms and automated desktop pools of full virtual machines as well as View Composer linked clones.
- When you want to remove a machine, `ViewDbChk` performs a health check on the machine and prompts you for additional confirmation if the machine looks healthy.
- `ViewDbChk` can delete erroneous or incomplete LDAP entries.
- `ViewDbChk` supports input and output using I18N character sets.
- `ViewDbChk` does not remove user data. For a full desktop virtual machine, `ViewDbChk` removes the virtual machine from inventory but does not delete it from disk. For a linked-clone desktop virtual machine, `ViewDbChk` deletes the virtual machine and archives the user disks to the root folder in the case of VMFS datastores or to a sub-folder named archiveUDD in the case of Virtual SAN and Virtual Volumes datastores.
- `ViewDbChk` does not support unmanaged desktop machines or RDS hosts in a manual farm.

ViewDbChk Syntax

```
ViewDbChk --findDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --enableDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --disableDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --findMachine --desktopName <desktop pool or farm name> --machineName <machine name>
[--verbose]

ViewDbChk --removeMachine --machineName <machine name> [--desktopName <desktop pool or farm
name>] [--force] [--noErrorCheck] [--verbose]

ViewDbChk --scanMachines [--desktopName <desktop pool or farm name>] [--limit <maximum deletes>]
[--force] [--verbose]

ViewDbChk --help [--commandName] [--verbose]
```

ViewDbChk Parameters

Parameter	Description
--findDesktop	Finds a desktop pool or farm.
--enableDesktop	Enables a desktop pool or farm.

Parameter	Description
--disableDesktop	Disables a desktop pool or farm.
--findMachine	Finds a machine.
--removeMachine	Removes a machine from a desktop pool or farm. Before removing a machine, `ViewDbChk` prompts the user to disable the desktop pool or farm. After removing the machine, `ViewDbChk` prompts the user to re-enable the desktop pool or farm.
--scanMachines	Searches for machines that are in an error or cloneerror state or have missing virtual machines, lists the problem machines grouped by desktop pool or farm, and gives the option to remove the machines. Before removing a machine, `ViewDbChk` prompts the user to disable the desktop pool or farm. After removing all erroneous machines in a desktop pool or farm, `ViewDbChk` prompts the user to re-enable the desktop pool or farm.
--help	Displays the syntax of `ViewDbChk`.
--desktopName <desktop name>	Specifies the desktop pool or farm name.
--machineName <machine name>	Specifies the machine name.
--limit <maximum deletes>	Limits the number of machines that `ViewDbChk` can remove. The default is 1.
--force	Forces machine removal without user confirmation.
--noErrorCheck	Forces the removal of machines that have no errors.
--verbose	Enables verbose logging.

Note All the parameter names are case-sensitive.

ViewDbChk Usage Example

A desktop machine named lc-pool2-2 is in an error state and we cannot remove it using View Administrator. We use ViewDbChk to remove it from the View environment.

```
C:\>viewdbchk --removeMachine --machineName lc-pool2-2
Looking for desktop pool "lc-pool2" in LDAP...
   Desktop Pool Name: lc-pool2
   Desktop Pool Type: AUTO_LC_TYPE
   VM Folder: /vdi/vm/lc-pool2/
   Desktop Pool Disabled: false
   Desktop Pool Provisioning Enabled: true
Looking for machine "/vdi/vm/lc-pool2/lc-pool2-2" in vCenter...
   Connecting to vCenter "https://10.133.17.3:443/sdk". This may take some time...
Checking connectivity...
   Connecting to View Composer "https://10.133.17.3:18443". This may take some time...
The desktop pool "lc-pool2" must be disabled before proceeding. Do you want to disable the
desktop pool? (yes/no):yes
Found machine "lc-pool2-2"
   VM Name: lc-pool2-2
   Creation Date: 1/25/15 1:20:26 PM PST
   MOID: vm-236
   Clone Id: b12a9ed2-8535-44ee-a9d6-6c9b5cf6f878
   VM Folder: /vdi/vm/lc-pool2/lc-pool2-2
   VM State: ERROR
Do you want to remove the desktop machine "lc-pool2-2"? (yes/no):yes
Shutting down VM "/vdi/vm/lc-pool2/lc-pool2-2"...
Archiving persistent disks...
Destroying View Composer clone "b12a9ed2-8535-44ee-a9d6-6c9b5cf6f878"...
```

```
Removing ThinApp entitlements for machine "/vdi/vm/lc-pool2/lc-pool2-2"...
Removing machine "/vdi/vm/lc-pool2/lc-pool2-2" from LDAP...
Running delete VM scripts for machine "/vdi/vm/lc-pool2/lc-pool2-2"...
Do you want to enable the desktop pool "lc-pool2"? (yes/no):yes
```

Further Troubleshooting Information

You can find further troubleshooting information in VMware Knowledge Base articles.

The VMware Knowledge Base (KB) is continually updated with new troubleshooting information for VMware products.

For more information about troubleshooting View, see the KB articles that are available on the VMware KB Web site:

http://kb.vmware.com/selfservice/microsites/microsite.do

Index